ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN
UNIVERSIDAD POLITÉCNICA DE CARTAGENA

Proyecto Fin de Carrera

Implementación de Mecanismos de Calidad de Servicio con Equipos Nortel

AUTORA: Sandra María García Pardo
DIRECTORAS: María Dolores Cano Baños
Cristina López Bravo

Septiembre / 2009

Autor	Sandra María García Pardo
E-mail del Autor	sgarciapardo2002@yahoo.es
Director(es)	María Dolores Cano Baños, Cristina López Bravo
E-mail del Director	mdolores.cano@upct.es
Codirector(es)	
Título del PFC	Implementación de Mecanismos de Calidad de Servicio con Equipos Nortel
Descriptores	

Resúmen

El ancho de banda en las redes es de vital importancia, ya que no es un recurso ilimitado. Los mecanismos de QoS es necesario implementarlos en cualquier tipo de red para proporcionar unos niveles de funcionamiento adecuados, al mismo tiempo que se maximiza eficazmente el reparto del ancho de banda del enlace, requerido por ciertas aplicaciones o especificado en un contrato del cliente con su proveedor de servicios (*Sevice Level Agreements, SLAs*). Solventar los nuevos requerimientos de Calidad de Servicio de las aplicaciones actuales será gestionando los recursos disponibles (el ancho de banda) de una forma eficiente.

El crecimiento que ha experimentado Internet en estos últimos tiempos ha incrementado la necesidad de proveer mayor número de servicios. Esta provisión tiene el problema de que la red debe permitir y garantizar el funcionamiento de los mismos; para conseguirlo, una de las formas más comúnmente usada es a través de políticas de Calidad de Servicio (QoS), aún así solamente el problema persiste cuando el proveedor o el cliente quieren verificar que el contrato se esté ofreciendo de forma correcta.

Esta verificación requiere que se analice la red de forma exhaustiva, para ello este proyecto propone un estudio de cómo implementar Calidad de Servicio con equipos Nortel, y un análisis y control de tráfico para determinar los cuellos de botella en el camino que siguen los paquetes y al mismo tiempo el impacto que recibe el usuario final.

Titulación	Ingeniería Técnica de Telecomunicación, especialidad Telemática
Intensificación	
Departamento	Tecnologías de la Información y las Comunicaciones
Fecha de Presentación	Septiembre – 2009

Índice

Índice Figuras

Índice Tablas

Acrónimos

- AF — Assured Forwarding (Servicio Asegurado)

- CA — Corriente Alterna (Alternating Current)
- CLI — Command Line Interface (Interfaz de Línea de Comandos)
- CPU — Central Process Unit (Unidad Central de Procesamiento)

- DiffServ — Differentiated Services (Servicios Diferenciados)
- DCE — Data-Circuit Terminating Equipment (Equipo de Comunicación de Datos)
- DTE — Data Terminal Equipment (Equipo Terminal de Datos)
- DSCP — Differentiated Services CodePoint
- DS Field — Campo DiffServ
- DVMRP — Distance Vector Multicast Routing Protocol (Protocolo de Encaminamiento Multicast en base a la Distancia de Vectores)

- ECN — Explicit Congestion Notification (Notificación Explícita de Congestión)
- EF — Expedited Forwarding (Tránsito expedito)

- FIFO — First-in first-out (Primero que llega, primero que sale)

- GUI — Graphic User Interface (Interfaz Gráfica de Usuario)

- ICMP — Internet Control Message Protocol (Protocolo de Mensajes de Control y Error de Internet)
- IGMP — Internet Group Management Protocol (Protocolo de Gestión de Grupos de Internet)
- IEEE — Institute of Electrical and Electronic Engineers (Instituto de Ingenieros Eléctricos y Electrónicos)
- IntServ — Integrated Services (Servicios Integrados)
- IP — Internet Protocol (Protocolo de Internet)
- IPG — InterPacket Gap (Tiempo de silencio entre tramas)
- IPX — Internetwork Packet Exchange (Intercambio de paquetes entre redes)

- LED — Light-Emitting Diode (Diodo Emisor de Luz)

- MAC — Medium Access Control (Dirección de Control de Acceso al Medio)
- MDI — Medium Dependent Interface (Interfaz Dependiente del Medio)
- MDI-X — Medium Dependent Interface – Crossover (Interfaz Cruzada Dependiente del Medio).

- OSPF — Open Shortest Path First (Primero la Ruta Más Corta)

- PC — Personal Computer (Ordenador Personal)
- PCMCIA — Personal Computer Memory Card International Association (Asociación Internacional de Tarjetas de Memoria para Ordenadores Personales)
- PHB — Per-Hop Behaviour (Comportamiento Por Salto)
- PTO — Packet Transmit Opportunity (Oportunidad de Transmisión de un Paquete)

- QoS — Quality of Service (Calidad de Servicio)

- RIP — Routing Information Protocol (Protocolo de Información de Encaminamiento)
- ROM — Read Only Memory (Memoria de Sólo Lectura)
- RSVP — Resource reSerVesion Protocol (Protocolo de Reserva de Recursos)

- SAP — Service Advertising Protocol (Protocolo de Publicación de Servicios)
- SDRAM — Synchronous Dynamic Random Access Memory (Memoria RAM Dinámica de Acceso Síncrono)
- SLA — Service-Level Agreement (Nivel de Servicio Acordado)
- SNMP — Simple Network Management Protocol (Protocolo Simple de Administración de Red)
- Strict PQ — Strict Priority Queueing (Encolamiento de Prioridad Estricta)
- Switch fabric — Tejido de Conmutación

- TCP — Transmission Control Protocol (Protocolo para el Control de la Transmisión)
- ToS Field — Type of Service Field (Campo Tipo de Servicio)

- UDP — User Datagram Protocol (Protocolo de Datagrama de Usuario)
- URL — Uniform Resource Locater (Localizador Uniforme de Recurso, Dirección de un Recurso de Internet)

- VLSM — Variable-Length Subreding Mask (Máscara de Subred de Longitud Variable)
- VoIP — Voice over IP (Voz sobre IP)

- WFQ — Weighted Fair Queing (Espera Equitativa Ponderada)
- WRR — Weighted Round Robin (Turno Rotativo Ponderado)

Capítulo 1

Introducción

1.1 Introducción

Según [1], [2], [3], [4], [5], [6], [7], [8], [9], [10] y [11], en la actualidad Internet puede definirse como una "mezcla de redes" con distintos anchos de banda y distintas características de retardo. Dentro de esta diversidad, unas partes de la red tendrán limitaciones de recursos que deberán ser provistas de forma eficiente, y por otro lado, otras partes de la red pueden estar provistas en exceso.

En la concepción inicial de Internet, la **idea** fue dotar de mayor inteligencia a los *hosts* extremos, y conceder de una **mínima capacidad de procesamiento a los routers**, ya que éstos sólo debían encaminar los datagramas sin ninguna acción adicional. Sin embargo, con la **aparición de nuevas aplicaciones de tiempo real**, como voz sobre IP (VoIP), telecontrol, videoconferencias, entre otras, Internet se quedaba obsoleta y por tanto, esta **visión** era inadecuada. Estas aplicaciones consumen gran ancho de banda, por ello es preciso añadir niveles de inteligencia que permitan **controlar los tráficos** asignando **prioridad al más crítico**. Por tanto, actualmente, se requiere de un tratamiento especial del tráfico **en cada nodo** de la red. Para ello, es necesario proponer y desarrollar nuevos modelos de arquitectura en la red, para que ésta pueda ofrecer este tratamiento diferencial de los datos y así, en el futuro, conforme crezca Internet, se asegure una buena Calidad de Servicio (QoS) a las aplicaciones en función de **"la importancia" de los datos** que se envíen por la red.

Según lo dicho, debido al aumento de la demanda (el número de usuarios) en Internet, crece la necesidad de que se creen **nuevos recursos** para mantener el ritmo de respuesta en las comunicaciones. Lo ideal, sería que **la red transporte el tráfico al ritmo al que las aplicaciones lo han generado.** Esto sólo sería posible si la disponibilidad de los recursos en la red fuera infinita. Sin embargo, la realidad consiste en todo lo contrario; **los recursos** en la red **son limitados**, y ésta es la razón por la que se dan los fenómenos de latencia, de **congestión** y de, por tanto, una posible pérdida de tráfico.

No todas las aplicaciones tienen la misma tolerancia a los retardos de tráfico y a las variaciones en la red. La presente demanda de las aplicaciones de voz, vídeo y datos, exige una mínima calidad de servicio, lo que nos lleva a una necesaria **administración eficiente de los recursos de la red**. Esta administración se lleva a cabo asignando distintos valores a los **parámetros de QoS** que cada aplicación requiere. Los parámetros que constituyen la base de la QoS, son:

- El retardo, también llamado latencia.
- Las variaciones del retardo: *jitter*.
- El ancho de banda.
- La pérdida de paquetes (o probabilidad de error).
- La disponibilidad, es decir, medir las interrupciones del servicio

Estos parámetros, son los "recursos a controlar" en la red. Si no existiese control de tráfico, se incrementaría la sensibilidad de **las aplicaciones multimedia** (voz y vídeo) a los retardos que se producen en la red. Esto se debe a que el protocolo IP ofrece un **servicio básico** conocido como **"*best effort*"**. Se trata de un servicio de encaminamiento no orientado a conexión. Sigue la filosofía de "se hace lo que se puede", encamina cada datagrama desde un origen a un destino **tan rápidamente como sea posible**. Como modelo de cola sigue el algoritmo FIFO, (primero que llega, primero que sale, *First-in, first-out*). *Best effort* equivale a decir "lo más posible, lo antes posible". Los paquetes con este tipo de servicio tienen la misma expectativa de tratamiento a medida que dichos paquetes transitan la red. Si llegase a ocurrir **congestión**, se **retardan** o **descartan** los paquetes. Esto hace muy escalable la red. Este servicio es idóneo para transportar las **aplicaciones tolerantes a la latencia**, tales como, el *correo electrónico, ftp, telnet, http*, donde el tiempo de envío y respuesta no es un problema importante.
Best effort no hace ninguna distinción entre cada aplicación, es decir, trata todo el tráfico por igual, y no garantiza la entrega eficaz que requiere el tráfico de **aplicaciones en tiempo real**, multimedia, de misión crítica, etc. Estas aplicaciones **no son compatibles** con este tipo de servicio.

Con todo esto, se concluye que a nivel IP no se tiene control sobre los parámetros de QoS, sólo se tiene *best effort* que no proporciona garantías de servicio (**retardo limitado y caudal**) a las aplicaciones de misión crítica. La forma de resolver esta dificultad, es mediante la definición de la Calidad de Servicio (QoS) requerida en la red.

1.2 Necesidad de Calidad de Servicio QoS

1.2.1 Definición de QoS

En el área de telecomunicaciones, QoS se define como el efecto global de las **prestaciones de un servicio** que determinan el grado de satisfacción de un usuario al utilizar dicho servicio. Desde el punto de vista de la red, la calidad ofrecida es el resultado de las **prestaciones ofrecidas** por cada una de las partes implicadas (terminales, la red de acceso, la red de transporte (*core*) y los servicios). La QoS está directamente relacionada con el tamaño de las colas y la congestión de la red, con la velocidad de conmutación y ancho de banda de los enlaces.

La QoS puede ayudar a mejorar el servicio que reciben los usuarios de la red, al mismo tiempo que reduce los costes de ofrecer dichos servicios. Para conseguir QoS en la red, se debe **administrar de manera "inteligente" el uso de los recursos** de la red, es decir, de forma "controlada" y "eficaz", para así no desperdiciar ancho de banda y utilizar la mínima cantidad posible de recursos hardware. En consecuencia **aumenta el rendimiento de la red** y **se evita** el **sobredimensionado**, esto es, la necesidad de **aumentar la capacidad** del ancho de banda. El aumento de la capacidad no es suficiente para evitar la congestión, ya que los datos se generan y se transmiten por **ráfagas**, lo cual implica que independientemente de la capacidad disponible, **siempre existirá congestión** al menos por breves períodos de tiempo. Además, hay que tener en cuenta que la mayoría de los protocolos de encaminamiento, aprenden los caminos para despachar los paquetes **sin considerar** los niveles de carga de los mismos. Otro punto crítico, es el **cuello de botella** de cualquier equipo extremo entre LAN y WAN donde el tráfico de LAN tiende a congestionar el enlace WAN aún en los enlaces de alta velocidad. Por tanto, el ancho de banda disponible no asegura un **retardo determinado o predecible**.

La QoS se basa en un conjunto de **técnicas y procedimientos** utilizados para dar un tratamiento preferente a unas clases de tráfico frente a otras, con el objetivo de cumplir unos requisitos mínimos en **parámetros** como el **retardo** o el **ancho de banda**. Es la habilidad de la red para ofrecer prioridad a unos determinados tipos de tráfico, sobre diferentes tecnologías (Frame Relay, ATM, LANs y líneas dedicadas).

Tras las explicaciones expuestas, se puede resumir que el **objetivo** de la Calidad de Servicio en una red es **cuantificar el tratamiento** que un paquete espera a medida que circula por la red; y que la QoS **no** puede crear **ancho de banda adicional**, sino que debe manejar el tráfico de manera que el ancho de banda disponible soporte los requerimientos de un amplio rango de aplicaciones que el funcionamiento del servicio *best effort* no puede soportar.
De este modo, **en situación de sobrecarga**, la QoS asegura que el tráfico crítico no sea **perdido** ni **retardado**.

1.2.2 ¿Por qué son necesarios los Mecanismos de QoS?

El tráfico en la red está formado por diferentes flujos de datos. A partir de un flujo de información dado, los **mecanismos de QoS** proporcionan a la red de datos la **capacidad** de asegurar, con un grado de fiabilidad preestablecido, que **se cumplan** los requisitos de tráfico necesarios en términos de **perfil** y **ancho de banda**, con el fin de conseguir **servicios útiles**.
En cada flujo, la **transmisión de paquetes en una dirección** tiene unas características significativas. Estas características pueden especificarse en términos de: caudal (*throughput*), retardo (*delay*), variación del retardo (*jitter*) y/o pérdidas. Los mecanismos de QoS miden, mejoran y garantizan dichas características a un nivel determinado. Por tanto, los datos en las grandes redes necesitan **control**.
Los mecanismos de QoS dividen el tráfico, de forma que se establecen "preferencias" en la asignación de los recursos de la red. Los mecanismos de control de tráfico tienen como fin hacer que Internet funcione con alto rendimiento, con capacidad de entregar máximo ancho de banda al tiempo que se ofrecen nuevos servicios y se reducen los costes de ofrecer dichos servicios.

Una **Red Inteligente** es una red con QoS. **Los mecanismos de QoS proveen** de mejores y más predecibles servicios a la red:

- Organizando el tráfico, esto es, identificando y priorizando los tráficos críticos.
- Evitando y manejando la **congestión de la red**.
- Mejorando las características de **pérdida de paquetes**.
- Dando a los usuarios **tiempos de respuesta más rápidos**.
- Mejorando el **uso del ancho de banda** existente.
- Añadiendo **fiabilidad** y **disponibilidad**.

Con el fin de cubrir las **necesidades presentes y futuras** de las aplicaciones y los tráficos multimedia.

1.2.3 Importancia del Ancho de Banda

El ancho de banda se puede definir como la cantidad de datos que se puede transmitir en un determinado periodo de tiempo, es decir, es la máxima cantidad de bits que pueden pasar por unidad de tiempo. Se expresa en bits por segundos.
El ancho de banda es importante porque describe las posibilidades de la red, de su capacidad de rendimiento, en términos del **tiempo de respuesta**. Si una determinada aplicación no dispone de un **mínimo de ancho de banda** para que su servicio sea llevado a cabo con eficacia, los usuarios se verán perjudicados. De este modo, los usuarios necesitan **priorizar y proteger** sus **aplicaciones de misión crítica** del tráfico de los restantes servicios que fluyen por la red y reducir los costes de las aplicaciones que no implican un tráfico crítico.
En consecuencia, es necesario administrar el **ancho de banda disponible** de manera eficiente con el objetivo de satisfacer las necesidades de las aplicaciones (demandas de los usuarios). Para ello, se debe **lograr QoS** en la red configurando los dispositivos de la red que implementen mecanismos de control de tráfico.

1.2.4 Configuración de los Dispositivos de QoS de la Red

Los dispositivos de la red, se intercambian tráfico mediante **interfaces**. Si la velocidad a la que el tráfico llega a una interfaz es superior a la velocidad que la interfaz puede enviar tráfico al siguiente dispositivo, se produce **congestión**. En esta situación, se utiliza QoS para tratar el tráfico y cumplir con los niveles de servicio, esto es, con los parámetros de QoS acordados en el contrato SLA (*Service Level Agreement*). La **capacidad de la interfaz** para enviar tráfico es por tanto un **recurso de red fundamental**, y su **asignación** viene determinada por los mecanismos de QoS.

Los pasos para asignar una capacidad específica a una interfaz de red son los siguientes:

1) **Clasificación de paquetes**: es el proceso de identificar y separar los diferentes flujos de datos que conforman el tráfico total que llega a los dispositivos de la red.
2) **Encolado**: el tráfico de cada flujo se envía a una cola de la interfaz de reenvío.
3) Determinación de la **velocidad** a la que se reenvía el tráfico de cada cola: las colas de cada interfaz se gestionan de acuerdo con el algoritmo de administración de cola configurado.

De esta forma, se determinan los recursos que se asignan a cada cola y a sus flujos correspondientes.

1.2.5 Arquitecturas de QoS

Entre los mecanismos de control de tráfico se distinguen dos modelos de arquitecturas para implementar Calidad de Servicio: la Arquitectura de Servicios Integrados (*IntServ*) y la Arquitectura de Servicios Diferenciados (*DiffServ*).

1.2.5.1 Arquitectura de Servicios Integrados (*IntServ*)

La arquitectura de Servicios Integrados se basa en la **pre-reserva de recursos** en los diferentes equipos de conmutación que componen el **trayecto** que seguirá la información en la comunicación, mediante un protocolo de *señalización* (RSVP, Protocolo de Reserva de Recursos). Por lo que convierte a IP hasta cierto punto en un "servicio orientado a conexión". El protocolo RSVP crea, mantiene y elimina cada reserva de recursos (**estados** en cada nodo), con el objetivo de proporcionar QoS extremo a extremo a un flujo determinado, y se encuentra tanto en los *hosts* extremos como en los routers.

El mecanismo de funcionamiento del protocolo de *señalización* RSVP, se resume en lo siguiente:

> Los *hosts* generarán *señalización* para una serie de aplicaciones específicas que incluyen aplicaciones multimedia y aplicaciones cualitativas de misiones críticas.
> Utiliza el ***host* extremo de transmisión** para **informar** de las características de QoS que requiere la aplicación.
> Utiliza el ***host* extremo de recepción** para realizar la **reserva de recursos** en la red.
> Los *routers* hacen uso de RSVP para **transportar los requerimientos de QoS** entre *routers* vecinos.
> De este modo, cada flujo de datos **crea un estado** en cada uno de los *routers* que atraviesan hacia su destino. En estos estados, se realizará una reserva de recursos necesarios para ofrecer QoS a las aplicaciones.

En resumen, cuando una aplicación realice una **petición de recursos**, esta solicitud atravesará todos los nodos que formen el trayecto para el flujo de información, y en función de los recursos disponibles será **aceptada o rechazada**. Por tanto, las dos funciones que debe realizar el modelo de servicios integrados son: la gestión de recursos y el control de admisión.

Los "Servicios Integrados" son complejos de implementar y pueden generar **mucho tráfico de señalización**, el cual, lleva a una **pobre escalabilidad** para el modelo de Servicios Integrados. Existirán aplicaciones para las que **la señalización** es menos útil. En especial, resulta ineficaz para aplicaciones que no están orientadas a conexión y que no generan flujos constantes, ya que se produce un **exceso de señalización**.
La gran cantidad de usuarios que componen una red, así como el **elevado número de flujos que puede generar cada usuario** provoca que existan graves problemas de escalabilidad en el núcleo de la red. Cada nodo de conmutación tiene que **almacenar un listado de todos los flujos activos y** los correspondientes **recursos asignados**. Por otro lado, estas **reservas son temporales** (*soft-state*) de manera que deben ser renovadas cada cierto tiempo.
Estos factores provocan que el modelo *IntServ* sea **difícilmente implementable** en una red de dimensiones considerables.

1.2.5.2 Arquitectura de Servicios Diferenciados (*DiffServ*)

La arquitectura de Servicios Diferenciados está fundamentada en la **priorización de clases de tráfico**. Se basa en la **separación** de los conceptos básicos de operación: reenvío (***forwarding***) y control (***routing***, encaminamiento), de los *routers*. En el reenvío, se realiza un **tratamiento diferenciado de los datagramas** PHB (*Per Hop Behaviour*), de acuerdo con la clase de tráfico. Así, las aplicaciones ya no tienen que realizar ninguna petición de recursos, como ocurre en el modelo *IntServ*, sino que se asignan prioridades a cada paquete de datos, para que sea tratado **por cada nodo** de manera diferente respecto a otros paquetes de datos.

Para la **identificación** de los **diferentes agregados de tráfico** se define un código llamado **DSCP** (*DiffServ Code Point*). Cada aplicación solicita un servicio **marcando** cada paquete con un **código** que indica el servicio deseado. DSCP forma parte del campo ToS de la cabecera de un paquete IP que permite la asignación de diferentes niveles de servicio al tráfico de la red.

La ventaja de *DiffServ* es que no utiliza ningún protocolo de señalización, no establece estados en cada nodo de la red. Por lo que es **más simple** que la arquitectura *IntServ* y presenta mejores condiciones para ser implantada en redes con grandes volúmenes de tráfico, es decir, **se escala mejor** en redes como Internet que la arquitectura *IntServ*.

Los **elementos de *DiffServ*** implementados en los nodos de la red son:

- **PHB**, *Per Hop Behaviour* en el reenvío: los paquetes se **clasifican y marcan** para recibir un **tratamiento específico por salto** en la ruta hacia su destino. *DiffServ* trata igual a los paquetes agregados de diferentes aplicaciones. En efecto, una vez que se marque el campo DS de un paquete con un valor DSCP adecuado, se trata igual que otros paquetes marcados con el mismo valor DSCP sin distinguir específicamente el origen de la aplicación.

- **Funciones de acondicionamiento** del tráfico como: clasificación, marcado y política de control, las cuales sólo se realizan en los **nodos frontera**:

  - **Clasificación**: Este proceso es necesario para que cada nodo sepa qué hacer con un paquete determinado entrante, esto es, **se determina el servicio PHB** que va a recibir cada paquete entrante al salir del nodo. En la clasificación **se identifican** qué aplicaciones han generado qué paquetes. La clasificación es pues la identificación de la **aplicación fuente** de cada paquete.

- **Marcado**: Proceso intensivo y complejo por lo que sólo debería realizarse una vez. Tras su identificación, el paquete se "marca" para asegurar que los conmutadores de la red sean capaces de darle prioridad. El tráfico transportado se marca a nivel IP, utilizando el campo DS (*DiffServ*). Esta información se mapeará en el campo **ToS** (*Type of Service*) de la cabecera de los paquetes IPv4, y en el campo ***Traffic Class*** de la cabecera de los paquetes IPv6.

- **Política de control**: se establece un Acuerdo del Nivel de Servicio SLA.

1.3 Objetivos del Proyecto

La ingeniería de tráfico es el proceso de **controlar** cómo fluye el tráfico a través de la red, con el fin de **optimizar** el uso de los recursos (ancho de banda de los enlaces) y **mejorar** el rendimiento de la red.

El proyecto consiste en dar QoS a la red de datos con congestión. En esta situación de cuello de botella, las prestaciones de la red se degradan y pierde calidad. Los equipos Nortel utilizados en este proyecto implementan el modelo de arquitectura *DiffServ*. La configuración de las herramientas *DiffServ* permite dar un trato "especial" al tráfico preferente y cumplir con los contratos SLA correspondientes de cada cliente.

Considerando todo lo anterior, los objetivos principales que se han marcado para este proyecto son los siguientes:

1. Implementación de Servicios Diferenciados en equipos Nortel.
2. Garantizar el ancho de banda contratado entre clientes y proveedores de servicios obteniendo información sobre la red mediante medidas realizadas con la ayuda de aplicaciones software.
3. Verificación de la Calidad de Servicio en diferentes entornos.
4. Estudiar cómo se realiza el reparto del ancho de banda en exceso.

Este proyecto **da un sólido entendimiento** de la instalación, configuración y administración de los conmutadores Nortel con capacidad de encaminamiento y de las habilidades necesarias para **cargar y para crear una configuración** básica, **ver estadísticas de administración** y **resolver problemas** de QoS.

1.4 Contenido del Documento

Este documento está estructurado en cuatro capítulos, incluyendo el presente, en los cuales se trata de dar una completa visión del trabajo realizado en este proyecto.
Como complemento a los capítulos se incluye un índice con las figuras y tablas incluidas, así como también, un resumen de los acrónimos utilizados.
Con el fin de facilitar la comprensión del documento, a continuación se proporciona una breve descripción de los capítulos que lo componen:

Capítulo 1: "Introducción"

Éste es el capítulo presente, en el cual, se plantea la necesidad de dotar de QoS a las redes actuales, se comparan las ventajas e inconvenientes entre los distintos modelos de arquitectura para implementar QoS, se marcan claramente los objetivos que se persiguen en el proyecto y se expone lo que se va a ver en cada capítulo.

Capítulo 2: "Calidad de Servicio en equipos Nortel"

En este capítulo se pretende mostrar el conjunto de herramientas con las que Nortel implementa la arquitectura de Servicios Diferenciados. Comienza con la presentación de un **manual** de usuario que explica la configuración inicial del equipo *Passport 8600 Routing Switch* para su puesta en marcha. Seguidamente, se explica cómo **configurar de manera general *DiffServ*** en el equipo *Passport 8600 Routing Switch* mediante el software de red *Device Manager* que los routers Nortel emplean para su configuración y funcionamiento. Esta configuración general incluye selección y configuración de puertos, definición de filtros y construcción de sets de filtros, definición y configuración de perfiles y políticas de descarte de paquetes.

Capítulo 3: "Pruebas experimentales"

Como su propio nombre indica, en este capítulo se expondrán las pruebas llevadas a cabo para probar las herramientas de *DiffServ* de Nortel y se comentarán los resultados experimentales obtenidos. Con estas pruebas se pretende mostrar las posibilidades que ofrecen los Servicios Diferenciados a la hora de garantizar contratos de una manera justa. Se analizará la influencia de los diferentes mecanismos de gestión y administración de colas en dichos contratos y en el reparto del ancho de banda en exceso de los enlaces.

Capítulo 4: "Conclusiones"

Este capítulo de cierre, aborda el análisis de los objetivos propuestos al inicio de este proyecto y de los resultados conseguidos a lo largo de su desarrollo.

Capítulo 2

Calidad de Servicio en equipos Nortel

2.1 Introducción

"NORTEL NETWORKS" es una de las multinacionales más importantes en el sector de las tecnologías de la información. Ha pasado de ser fabricante pionero de teléfonos, que atendía principalmente al mercado canadiense, a convertirse en uno de los proveedores globales más grandes del mundo de redes de datos avanzadas.

Para comenzar este capítulo, según [2], [12], [13] y [14], se presenta un **manual de usuario** que explica la **configuración inicial** del equipo *Passport 8600 Routing Switch* (ver figura 2.1).

Figura 2.1: *Passport 8600 Routing Switch*

Seguidamente, según [15], [16], [17] y [18], se explica cómo **configurar de manera general *DiffServ*** en el equipo *Passport 8600 Routing Switch*. Esta configuración general incluye **definición de filtros**, **asignación de ancho de banda**, **definición de perfiles** y **políticas de descarte de paquetes**.

2.2 Configuración Inicial del router Passport 8600 Routing Switch

Las series *Passport 8600 Routing Switch* son una familia de *routers* modulares de acceso multiservicio, pertenecientes a la multinacional canadiense *Nortel Networks*, que proporcionan una conexión eficaz entre **redes de datos de última generación**.
Su diseño ofrece estrategias de conexión en múltiples niveles y un alto grado de rendimiento, escalabilidad, fiabilidad y Calidad de Servicio (*QoS*).
Los *routers Passport 8600 Routing Switch* combinan las capacidades para trabajar tanto a nivel 2 (capa de enlace) como a nivel 3 (capa de red).
Los módulos de estos conmutadores con capacidad de encaminamiento, proporcionan una retransmisión de paquetes a muy alta velocidad. Esta retransmisión, se vale del protocolo *IP* (*Internet Protocol*) y del protocolo IPX (*Internetwork Packet Exchange*, Protocolo para el Intercambio de Paquetes entre redes) para llevar a cabo el proceso de encaminamiento.

La **arquitectura** del *Passport 8600 Routing Switch* consta de los siguientes elementos:

- Chasis *Passport* de la serie *8000*
- Fuentes de alimentación CA *Passport 8001PS*

- Módulos de conmutación *Passport* de la serie *8600*
- Guía de cables
- Unidades de ventilación

Concretamente, el chasis del equipo es el ***Passport 8006 Chassis***. En él, se pueden instalar hasta tres fuentes de alimentación y hasta seis módulos de conmutación. Dependiendo del número de módulos y de fuentes de alimentación instalados/as en el equipo, se puede optar por realizar sobre éste una **configuración redundante** o una configuración no redundante. Así, se asegura una **alta fiabilidad** gracias a la réplica de recursos:

- Si el número de módulos instalados es de **cinco o menos**, sólo se requiere de una fuente de alimentación CA (Corriente Alterna) para una configuración no redundante. Si se desea una configuración redundante, se deben instalar dos fuentes de alimentación.
- Si el número de módulos instalados es de **más de cinco**, se requiere de un mínimo de dos fuentes de alimentación para una configuración no redundante. Una configuración redundante implica el uso de tres fuentes de alimentación.

En este sistema, sólo hay una fuente de alimentación (ver figura 2.2), la cual suministra la energía que el sistema necesita, y dos módulos instalados, con lo cual, se trabajará con una **configuración no redundante**.

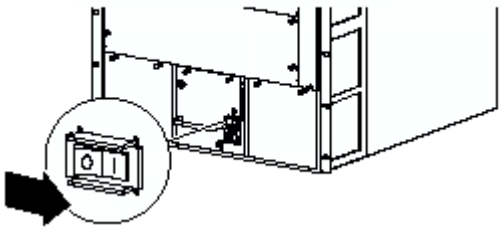


Figura 2.2: Fuente de Alimentación CA

Respecto a los módulos de conmutación, existen dos variedades**: módulos de entrada/salida** y **módulos *switch fabric***. Entre los módulos de entrada/salida se distinguen ocho módulos diferentes. Sin embargo, se dispone de un solo tipo de módulo *switch fabric*.

- El módulo *switch fabric* (tejido de conmutación) es el cerebro del *router*. Este módulo tiene reservados los *slots* o ranuras 5 y 6 del chasis.

- Los módulos de entrada/salida tienen la funcionalidad de recibir y reenviar la información que les llega de los *hosts* que constituyen las distintas redes de datos conectadas al *router*. Estos módulos sólo se pueden instalar en los cuatro primeros *slots* del chasis.

Así, en el *Passport 8006 Chassis*, se pueden instalar hasta un máximo de cuatro módulos de entrada/salida y un máximo de dos módulos *switch fabric*.

El *Passport 8600 Routing Switch* con el que se va a trabajar, dispone de los siguientes módulos de conmutación:

- **Passport 8690SF Module**: 1 módulo *switch fabric* (ver figura 2.3)
- **Passport 8648TXE Module**: 1 módulo de entrada/salida (ver figura 2.4)

Figura 2.3: *Passport 8690SF Module*

Figura 2.4: *Passport 8648TXE Module*

Otro de los elementos instalados en el chasis, es la guía de cables (ver figura 2.5). Ésta facilita las operaciones de cableado, ya que permite encaminar los cables que se conectan a los distintos módulos.

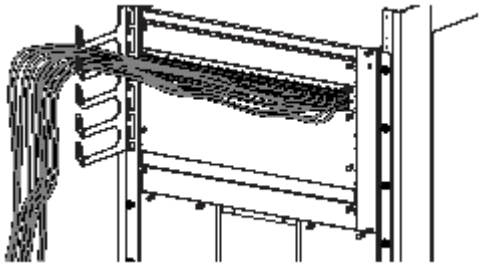


Figura 2.5: Guía de Cables

Por último, el chasis consta de dos unidades de ventilación que proporcionan una correcta refrigeración del dispositivo.

Una vez montado todo el equipo, es necesario **configurar el *router*** antes de que sea incorporado a la red de datos. Este manual proporciona la información necesaria para realizar la configuración inicial.

2.2.1 Capacidades del *router Passport 8600 Routing Switch*

Las distintas capacidades o funcionalidades implementadas en el *router*, vienen determinadas por las características de los módulos que estén instalados. Como se ha comentado en la sección anterior, el equipo del que se dispone en el laboratorio consta de dos módulos de conmutación: el *Passport 8690SF Module* y el *Passport 8648TXE Module*.

Las prestaciones que ofrece este conmutador en particular se pueden resumir en:

- Capacidad de 64 gigabits (Gb) y de 10 megabytes (MB) de memoria por cada módulo 8690SF.

- Soporte para los protocolos de encaminamiento: RIP, RIP2, OSPF, IGMP, DVMRP, IPX-RIP y IPX-SAP.

- Hasta 1979 VLANs definidas por puerto o por política (protocolo, MAC origen, o subred *IP*) y hasta 500 rutas.

- Mecanismos de Calidad de Servicio sobre una arquitectura de Servicios Diferenciados basados en hardware: **8 niveles de QoS**.

- Estándar IEEE 802.1Q: protocolo de LAN que permite etiquetar cada trama *Ethernet* para crear VLANs entre varios *switches*. El conmutador dispone de múltiples bases de datos para tal proceso.

- Estándar IEEE 802.1d: protocolo de LAN que permite crear de forma automática un árbol lógico de conexiones (*Spanning Tree*), en vez de usar los *loops* físicos que pueden provocar que la red se inunde. De esta forma, se evita que llegue un momento en que ninguna estación pueda transmitir.

- **Estándar IEEE 802.1p**: protocolo de LAN que permite tratar de forma selectiva las tramas, asignándoles prioridades, para incorporar aplicaciones en tiempo real en *Ethernet*.

- Uso de los protocolos IGMP (*Internet Group Management Protocol*, Protocolo de Gestión de Grupos de Internet) y DVMRP (*Distance Vector Multicast Routing Protocol*, Protocolo de Encaminamiento Multicast en base a la Distancia de Vectores) para la optimización de una configuración Multicast *IP*.

- Soporte para puertos *router* virtuales sin degradación en la funcionalidad.

- Soporte completo para Máscara de Subred de Longitud Variable (VLSM, *Variable-Length Subreding Mask*) en *software* y en *hardware*.

- Asignación flexible de rutas estáticas.

- Soporte para **puertos *"brouter"*** (*bridge* + *router*) que permiten que un puerto físico sea usado tanto por protocolos de encaminamiento (*routing*) como por protocolos que no son de encaminamiento (*bridging*).

- Configuración de **direcciones *supernet*** sobre interfaces *router* virtuales, y de direcciones *supernet* que se han aprendido usando un protocolo dinámico de encaminamiento.

- Filtrado de paquetes *IP* mediante *hardware* con un impacto mínimo en la latencia entre tramas filtradas y no filtradas.

- Tramas de hasta 1950 bytes sobre puertos *Ethernet* de 10/100 megabits (Mb).

- Tres posibilidades para la gestión y administración del *router*: *software* **Device Manager**, navegador **Web** y la interfaz de línea de comandos (**CLI**).

2.2.2 Módulos de Conmutación *Passport 8600*

2.2.2.1 Módulo *Switch Fabric* "Passport 8690SF Module"

El módulo *Passport 8690SF* es la parte más importante de la arquitectura del *router Passport 8600 Routing Switch* (ver figura 2.6).

En la tarjeta 8690SF destacan los siguientes elementos:

- Núcleo *switch fabric*
- Subsistema CPU
- Reloj de tiempo real

- El **núcleo** o *kernel* es la pieza clave para realizar la función principal del *router*, es decir, realiza el encaminamiento conmutando todo el tráfico que pasa por los módulos de entrada/salida 8600.

- El **subsistema CPU**, lleva a cabo la gestión entre el módulo *switch fabric* y los módulos de entrada/salida. Este subsistema está constituido por:

  - Microprocesador *PowerPC*.
  - Memoria de sistema (SDRAM) de 64 MB. Almacena tablas de encaminamiento.
  - Memoria Flash de 16 MB. Carga los archivos de imagen.
  - Memoria ROM de 2 MB. Gestiona el proceso de arranque.
  - Tarjeta PCMCIA de Memoria Flash. Almacena configuraciones del *switch* y carga archivos de imagen. Debido a su portabilidad, facilita el intercambio de archivos entre varios *routers*.

Además, el módulo *switch fabric* se basa en 10 MB de memoria compartida de alta velocidad que almacena el tráfico **"procedente de"** o **"con destino a"** los módulos de entrada/salida. El conmutador asigna memoria a las diferentes **colas de paquetes de datos**, que tienen establecidas distintas prioridades, según la **utilización** del tráfico y la configuración actual del conmutador.

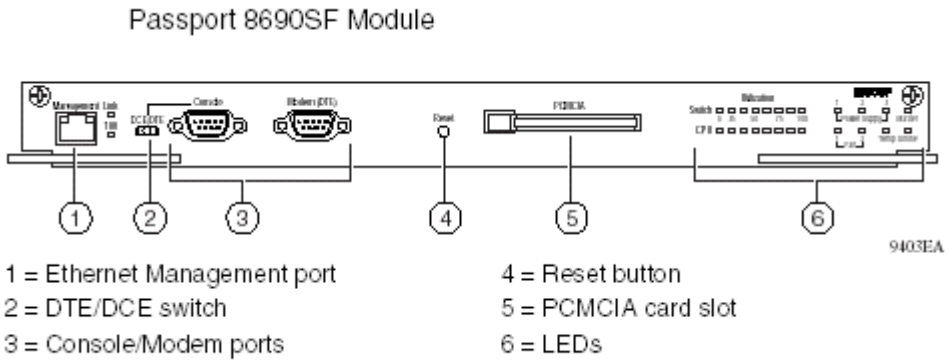


Figura 2.6: Vista del Panel Frontal del *Passport 8690SF Module*

Las características físicas del *panel frontal* del módulo *Passport 8690SF* incluyen:

- **Puerto de Gestión *Ethernet***: MDI (*Medium Dependent Interface*) 10/100BASE-T y conector RJ-45. Permite la gestión del equipo a través de un navegador Web, el *software Device Manager* o mediante una sesión Telnet para acceder a la CLI (Interfaz de la Línea de Comandos). Se le debe asignar una dirección *IP*.

- **Interruptor DTE/DCE**: cambia la asignación de pines del puerto serie de la consola. De esta forma, ésta puede operar como un dispositivo DTE (Equipo Terminal de Datos, *Data Terminal Equipment*) o como un dispositivo DCE (Equipo de Comunicación de Datos, *Data-Circuit Terminating Equipment*).

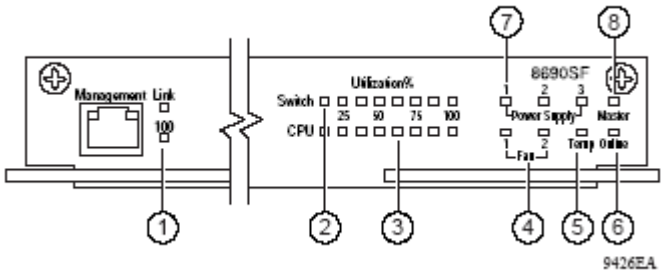
- **Puertos Serie**: cable RS-232 y conector DB-9.

    - **Puerto de la Consola** → acceso al módulo *switch fabric* desde un terminal utilizando la interfaz de la línea de comandos.
    - **Puerto de Módem** → permite una administración "*dial-up*" (marcado manual) del *router* a través de la conexión de un módem estándar.

- **Botón *Reset***: posibilita una reposición al estado inicial del *hardware* o reiniciar el sistema.

- **Ranura PCMCIA**: para Tarjeta de Memoria Flash (8M) ATA-Sandisk del tamaño de una tarjeta de crédito, que proporciona un modo rápido para la transferencia de configuraciones entre múltiples conmutadores, o para la carga de múltiples configuraciones para un único conmutador.

- **Indicadores LED**: indican **el estado** de los subsistemas del módulo, de las fuentes de alimentación y de las unidades de ventilación del equipo (ver figura 2.7).



1 = Indicadores LED del puerto de gestión
2 = Indicadores LED de utilización del conmutador
3 = Indicadores LED de utilización de la CPU
4 = Indicadores LED de ventilador
5 = Indicador LED de temperatura
6 = Indicador LED de «en línea»
7 = Indicadores LED de alimentación
8 = Indicador LED maestro

Figura 2.7: Indicadores LED del Módulo 8690SF

- El estado de los subsistemas se muestra en:

    - Los 8 LEDs que indican el ***porcentaje de la utilización*** del conmutador (**Switch**). Podemos distinguir hasta 8 niveles dependiendo del número de LEDs encendidos:

1 LED = 10 Mb/s	5 LEDs = 10 Gb/s
2 LEDs = 100 Mb/s	6 LEDs = 20 Gb/s
3 LEDs = 1 Gb/s	7 LEDs = 40 Gb/s
4 LEDs = 5 Gb/s	8 LEDs = 64 Gb/s

    - Los 8 LEDs que indican el ***grado de actividad*** de la **CPU**. Éste variará en función del número de tareas que se estén ejecutando. Las tareas que la CPU realiza son: el aprendizaje de direcciones MAC, la actualización de las tablas

de encaminamiento, además de interactuar con la estación que gestiona y administra el *router*. Podemos distinguir hasta 8 niveles de actividad dependiendo del número de LEDs encendidos:

1 LED = 12%	5 LEDs = 60%
2 LEDs = 24%	6 LEDs = 72%
3 LEDs = 36%	7 LEDs = 84%
4 LEDs = 48%	8 LEDs = 100%

- LEDs del Puerto de Gestión:
  - **Link** → indica su estado de enlace, esto es, si hay o no conexión.
    - **Off** (apagado): no hay enlace.
    - **Verde/fijo**: puerto conectado y enlace estable.
  - **100** → indica su velocidad de operación.
    - **Off**: 10 Mbps.
    - **Verde/fijo**: 100 Mbps.
- LED **Master** (Maestro):
  - **Off**: subsistema CPU evaluando la existencia o no de problemas en el sistema.
  - **Verde/fijo**: subsistema CPU preparado y en modo de espera.
  - **Verde/intermitente**: se están proporcionando funciones de CPU activas al conmutador.
  - **Ámbar/fijo**: subsistema CPU averiado.
- LED **Online** (En línea):
  - **Off**: *switch fabric* offline.
  - **Verde/fijo**: *switch fabric* online.
  - **Ámbar/fijo**: comprobación de fallos del *switch fabric* no superada.

➢ El estado de la fuente de alimentación se muestra en:

- LEDs **Power Supply** (Alimentación):
  - **Off**: fuente de alimentación no encendida o no hay fuente de alimentación en la posición especificada.
  - **Verde/fijo**: estado de operación normal.
  - **Ámbar/fijo**: fuente de alimentación averiada.

➢ El estado de las unidades de ventilación se muestra en:

- LEDs **Fan** (Ventilador):
  - **Verde/fijo**: estado de operación normal.
  - **Ámbar/fijo**: unidad de ventilación averiada.
- LED **Temp** (Temperatura):
  - **Verde/fijo**: la temperatura es normal para la operación del *switch*.
  - **Ámbar/fijo**: temperatura máxima de operación excedida.

2.2.2.2 Módulos Passport 8600 de entrada/salida

Los módulos de entrada/salida se encargan de recibir y de reenviar los diferentes paquetes que le llegan de los *hosts* pertenecientes a las distintas redes de datos conectadas al *router*.

La **arquitectura general** de estos módulos consta de los siguientes elementos:

- Placa de circuitos de reenvío
- Panel frontal

- **La placa de circuitos de reenvío** contiene el **"motor de transporte"**, "**unidades de resolución de direcciones"** y **"colas de salida"**. Su funcionalidad consiste en encaminar el tráfico hacia el módulo *switch fabric*.
  El almacenamiento local de los datos transportados permite que *el motor de transporte* resuelva direcciones y reenvíe los paquetes a través del módulo *switch fabric* sin la intervención de la CPU.
  El *motor de transporte* también filtra paquetes según las **políticas de priorización** establecidas. Con lo cual, se garantiza por adelantado **"servicio ininterrumpido"**, cuando sea necesario, para **"aplicaciones críticas"**, es decir, para aplicaciones que requieren un gran ancho de banda. La información de priorización se establece en las **cabeceras de los paquetes**. Por cada puerto, hay ocho niveles de priorización de colas. Para la asignación de prioridades a los distintos flujos de aplicaciones que van llegando al *router*, éste se puede configurar para operar en modo ***Strict PQ*** (***priority queueing***), o bien bajo la disciplina de servicio ***WFQ*** (***Weighted Fair Queing***).
  Existe un '*buffer*' de salida de 4 MB de capacidad de memoria. Estos 4 MB de memoria pueden estar asignados a cada puerto Gigabit *Ethernet*, en los módulos que dispongan de un medio de transmisión de fibra óptica o bien compartidos entre 8 puertos de 10/100 Mbps en los módulos *Fast Ethernet*. El módulo de entrada/salida *Passport 8648TXE* es un módulo *Fast Ethernet*.

- **El panel frontal** consta de los dispositivos de la capa física (medios de transmisión), incluyendo los controladores MAC (Control de acceso al medio, *Media Access Control*).

2.2.2.2.1 Módulo de entrada/salida "Passport 8648TXE Module"

El módulo *Passport 8648TXE* es un módulo de entrada/salida *Fast Ethernet*. Este es el módulo de entrada/salida instalado en el equipo del laboratorio (ver figura 2.8).

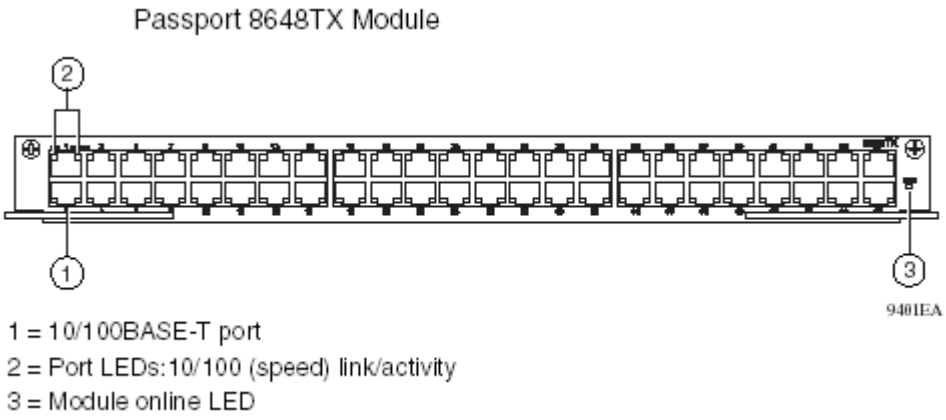


Figura 2.8: Vista del Panel Frontal del *Passport 8648TXE Module*

La tarjeta *Passport 8648TXE* lleva a cabo una negociación automática con el dispositivo remoto conectado, para conseguir la mayor tasa de datos posible, y un convenio en el modo de operación para recibir/transmitir la información (*half-duplex* o *full-duplex*).

Como podemos observar en la figura, los elementos que se muestran en el panel frontal de este módulo de entrada/salida son los siguientes:

- Puertos
- Indicadores LED

- Las características físicas de los **puertos** son:

  - Número: 48.
  - Tipo de conector: RJ-45 cableados como MDI-X (*Medium Dependent Interface - Crossover*).
  - Alcance: hasta 100 metros por segmento.
  - Velocidad: 10/100 Mbps.
  - Modo de operación: full-duplex ó half-duplex.

- **Indicadores LED**: indican el estado de los puertos y el correcto funcionamiento o no del módulo (ver figura 2.9).

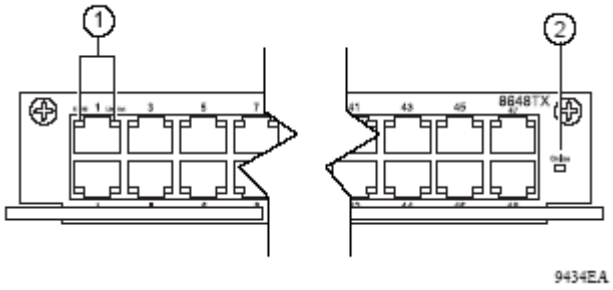


Figura 2.9: Indicadores LED del Módulo 8648TXE

- El estado de cada puerto se muestra en:

  - Indicadores LED de puerto:

    - **10/100** → indica su velocidad de operación.
      - **Off** (apagado): 10 Mbps.
      - **Verde/fijo**: 100 Mbps.

    - **Link/Act** (Enlace/Actividad) → indica el estado del enlace y la actividad del puerto.
      - **Off**: puerto inhabilitado ó no tiene enlace.
      - **Verde/fijo**: puerto conectado y enlace estable.
      - **Verde/ intermitente**: transferencia de datos.

- El estado del módulo se muestra en:
    - Indicador LED **Online** (En línea) que indica el estado de funcionamiento del módulo:
        - **Off**: módulo apagado o módulo encendido en estado no funcional, es decir, en estado de la auto-comprobación de encendido y de la inicialización del *software*.
        - **Verde/fijo**: estado de funcionamiento normal tras completar con éxito la auto-comprobación de encendido y la inicialización del *software*.
        - **Ámbar/fijo**: el módulo no ha pasado la auto-comprobación de encendido.

2.2.3 Puesta en Marcha del Equipo

Una vez descritos con detalle los módulos que constituyen el equipo del laboratorio, se describirá cómo poner en marcha el *router* por primera vez antes de que sea incorporado a la red (*network*).
En este apartado, se puntualizará cómo dar una configuración básica utilizando para tal fin *la interfaz de línea de comandos* (CLI). Esta configuración inicial, deberá incluir la asignación de una **dirección *IP*** al equipo.
Una vez que el *router* tenga configurada su dirección *IP*, se puede configurar y administrar más fácilmente utilizando el *software* **Device Manager**. Este programa proporciona un entorno de trabajo más adecuado y comprensible que el uso de la *interfaz de línea de comandos* (CLI), la cual implica el aprendizaje del formato de los numerosos comandos que engloban todas las opciones y capacidades que ofrece el *Passport 8600 Routing Switch*.

PASO1: Acceder al *Router*.

El acceso al *router* se lleva a cabo desde un *PC*. Dicho acceso puede hacerse de forma local o de forma remota a través de una ***conexión módem***.
El *acceso local* se realiza a través del Puerto de la Consola. El *acceso remoto* se realiza a través del Puerto de Módem. Ambos puertos series están localizados en el módulo *switch fabric*.
Para la conexión del terminal (*PC*) a dichos puertos se usa un cable *null-módem* RS-232 con conector DB-9. De esta forma, se puede establecer con el *router* una **sesión de emulación de terminal** desde un *PC*.
El programa que nos permite establecer la sesión es **HyperTerminal**, que es una aplicación accesoria en Microsoft Windows. Para abrir HyperTerminal, haga clic en "Inicio", seleccione "Programas", "Accesorios", "Comunicaciones" y, a continuación, haga clic en "HyperTerminal".
Este *software* de comunicaciones permite ***intercambiar información*** y transferir ficheros entre distintos dispositivos que dispongan de conexión serie RS-232.

Una vez que el *PC* está conectado desde uno de sus puertos de comunicaciones al Puerto de la Consola del *router*, se deben seguir los siguientes **pasos** para crear una sesión:

- Ejecutar el programa HyperTerminal.
- Iniciar nueva conexión. Asignarle un nombre.
- Indicar el puerto de comunicaciones que se está utilizando: COM1, COM2.
- Paso más importante: ***Configuración del puerto de comunicaciones*** al que asignamos las siguientes propiedades (ver figura 2.10):
    1. Bits por segundo: 9600.
    2. Bits de datos: 8.
    3. Paridad: Ninguna.
    4. Bits de parada: 1.
    5. Control de flujo: Ninguno.
- Aceptar.

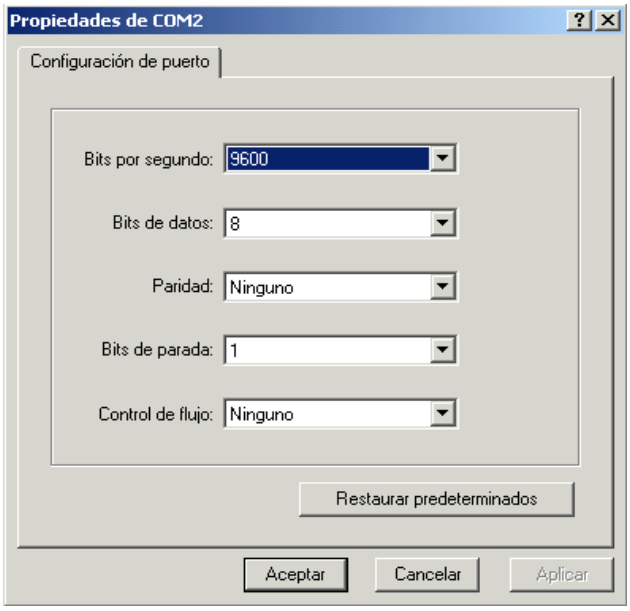


Figura 2.10: Configuración del Puerto de Comunicaciones

Tras crear una sesión, puede desconectarse o volverse a conectar haciendo clic en los iconos de desconexión y conexión respectivamente. También puede grabar la salida de una sesión seleccionando "Archivo → Guardar". Las sesiones serán guardadas en la carpeta de "HyperTerminal" con el nombre que le asignó y así, no tendrá que volver a configurar sucesivas sesiones.

Tras el establecimiento de sesión de emulación de terminal, cuando se enciende el *router*, nuestro *PC* muestra por pantalla la información de la auto-comprobación de encendido y de la inicialización del *software* del *router*. Una vez finalizados con éxito estos procesos, se tiene acceso a la *interfaz de línea de comandos* (CLI) mediante la cual, se configurará el *router* por primera vez introduciendo por teclado los comandos que se requieran.

PASO2: Encender el *Router*.

Entre las dos posibilidades de acceso al *router*, se ha decidido optar por un acceso local. Por tanto, se usará el Puerto de la Consola del módulo *switch fabric* para gestionar la configuración básica.
Un *PC* es un dispositivo DTE (Equipo Terminal de Datos). Además, el cable que une el *router* con el *PC* es un cable **null-módem** (supresor de módem). Así, se establece una **conexión DTE-DTE**. En consecuencia, antes de encender el *router*, se debe comprobar que el **"interruptor DTE/DCE"** del módulo *switch fabric* está en modo DTE (hacia la derecha, ver figura 2.11), para que el *router* actúe como equipo terminal de datos DTE.

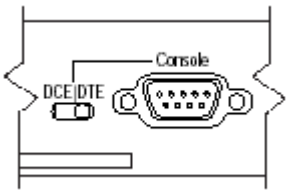


Figura 2.11: "Interruptor DTE/DCE en modo DTE"

Cuando el *router* se pone en marcha, ejecuta su ***proceso automático de arranque***. Localiza el *hardware*, esto es, los módulos instalados en el chasis, y realiza una serie de rutinas de ***detección*** del mismo. Ejecuta diagnósticos desde la memoria ROM y la memoria *flash* en todos los módulos *hardware*. Estos diagnósticos verifican el funcionamiento básico de su CPU, de su memoria y de los puertos de interfaz. Una vez que el *hardware* se muestra en una ***disposición de funcionamiento*** correcta, el dispositivo continúa con la inicialización del *software*, es decir, lleva a cabo ***rutinas de inicio del sistema***. Tras cargar el sistema operativo, el dispositivo trata de localizar y aplicar la ***configuración*** disponible en la memoria *flash*.

La CLI consta de dos sistemas de comandos a los que se accede de diferentes formas:

- Comandos ***Boot Monitor* CLI** → sirven para configurar las opciones de arranque del *router* y gestionar los archivos almacenados en la memoria *flash*.

- Comandos ***Run-Time* CLI** → sirven para configurar las operaciones del *router* y el acceso de la administración y gestión del mismo.

La "secuencia de arranque" que sigue el conmutador, está establecida por defecto y consiste en la carga de una serie de archivos ejecutables de extensión **.img** y de configuración de extensión **.cfg**. Para modificarla, se debe entrar al sistema como ***boot monitor*** (ver figura 2.12). Para acceder, se debe presionar **"enter"** antes de que pasen los primeros cuatro segundos de la secuencia de arranque. De esta forma, el proceso de auto-arranque se detendrá inmediatamente y entraremos en el sistema en modo *boot monitor*. El '*prompt*' del sistema estará representado como: **monitor#**.

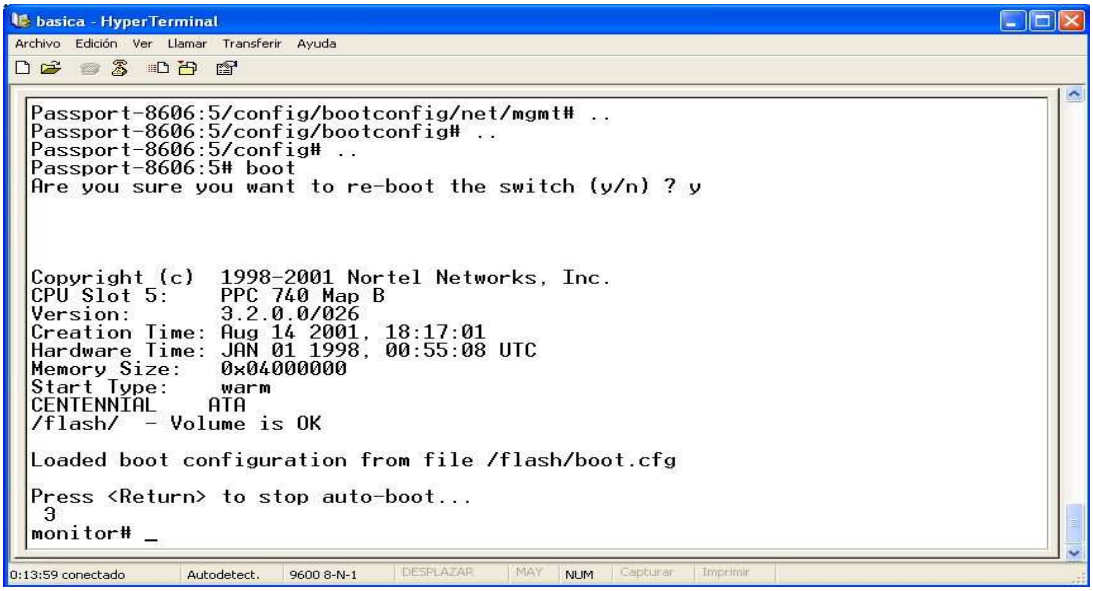


Figura 2.12: Acceso al Sistema en modo *Boot Monitor* CLI

Para obtener información y poder cambiar el orden de arranque del sistema, la *Boot Monitor* CLI dispone de los comandos ***choice***, los cuales son exclusivos de ésta. Para salvar la configuración de arranque es necesario introducir el siguiente comando antes de salir del sistema *Boot Monitor*:

- **save**

Los comandos *Boot Monitor* CLI, tienen su equivalente en los comandos *config bootconfig* de la *Run-Time* CLI.

Nota: Cuando se está en modo *Run-Time* CLI, se pueden usar los comandos *config bootconfig* para hacer cambios de configuración en la *Boot Monitor* CLI. Para que dichos cambios queden reflejados, es necesario introducir el siguiente comando antes de salir del sistema *Run-Time*:

- **save bootconfig**

Si no se detiene la secuencia de arranque, es decir, si no se pulsa **"enter"** antes de que pasen los primeros cuatro segundos, ésta se completará.
Una vez que el conmutador haya finalizado su secuencia de arranque, se puede acceder a la *Run-Time* CLI introduciendo previamente un nombre de usuario (*login*) y su *password* correspondiente (ver figura 2.13).
El '*prompt*' del sistema estará representado como: **Passport-8006:5#**. El final del '*prompt*' indica el número del *slot* del *chasis Passport 8006* donde está instalado el módulo *switch fabric* 8690SF.

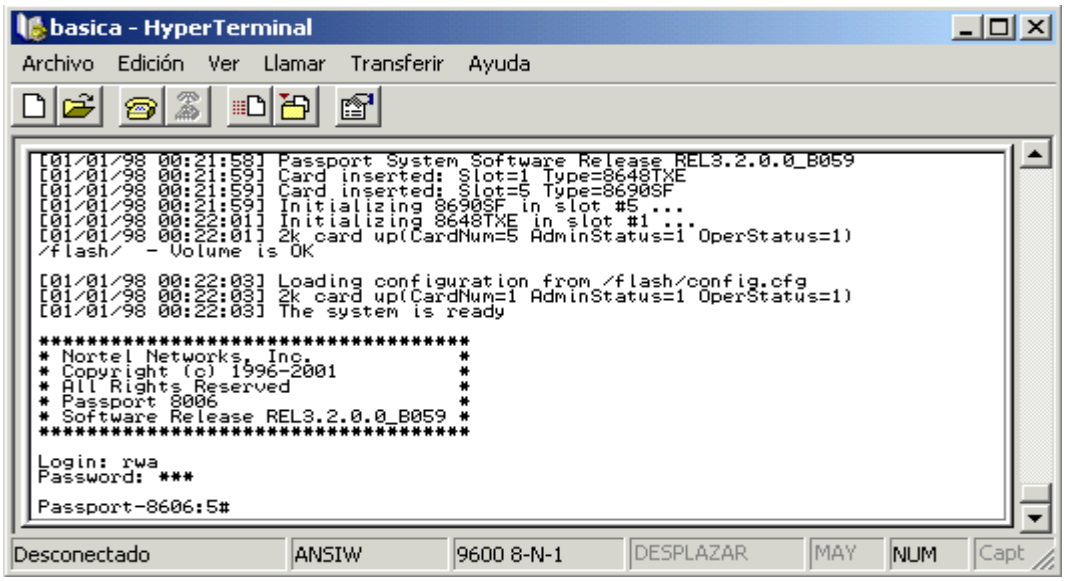


Figura 2.13: Acceso al Sistema en modo *Run-Time* CLI

Los comandos *Run-Time* CLI permiten la ejecución de la mayor parte de las funciones de configuración y de gestión para administrar el conmutador.

PASO3: Entrar al Sistema.

El *router* posee una estructura de **seguridad de acceso** al sistema. Este sistema de seguridad es necesario para restringir el acceso a las funciones de gestión y de administración del conmutador.
Existen hasta ***seis niveles de acceso*** diferentes. Cada nivel se diferencia de los otros por los permisos que tienen para poder realizar ciertas funciones de gestión del dispositivo.

Tabla 2.1: Niveles de acceso y enumeración de sus correspondientes *logins* y *passwords*

Nivel de acceso	Descripción	Login por Defecto	Password por defecto
sólo-lectura	Permite únicamente la lectura de información de estado y de configuración.	ro	ro
capa1 (lectura/escritura)	Permite ver la información de estado y de configuración del conmutador y cambiar los parámetros de las interfaces.	L1	l1
capa2 (lectura/escritura)	Permite ver y cambiar la configuración y la información de estado de funciones propias del nivel 2 (*bridging/switching*).	L2	l2
capa3 (lectura-escritura)	Permite ver y cambiar la configuración y la información de estado de funciones propias del nivel 2 (*bridging/switching*) y del nivel 3 (*routing*).	L3	l3
read/write (lectura/escritura)	Permite ver y cambiar la configuración y la información de estado a través del *switch*. No se puede cambiar los ajustes de seguridad (*passwords*) establecidos.	rw	rw
read/write/all (todos)	Se tienen todos los privilegios de acceso lectura-escritura y la capacidad para cambiar los ajustes de seguridad (nombres de usuario (*logins*) y las *passwords*), incluyendo la gestión basada en Web.	rwa	rwa

Para acceder a *Run-Time* CLI, es necesario introducir un nombre de usuario (*login*) y su clave de acceso (*password*) asociada. El *router* tiene establecidos unos *logins* y unas *passwords* por defecto (ver tabla 2.1). Después de haber entrado por primera vez al sistema, se puede establecer nuevos *logins* y *passwords* siempre y cuando se haya accedido a la *Run-Time* CLI teniendo permisos de **lectura/escritura/todos** (rwa). Se debe tener en cuenta que el establecimiento de nuevos *logins* y *passwords* no puede realizarse desde la *Boot Monitor* CLI, únicamente es posible si se ha accedido en modo *Run-Time*.

El cambio de los nombres de usuario (*logins*) y de las claves de acceso (*passwords*) se realiza introduciendo:

- **config cli password ro <username> [<password >]**; cambia el *login* y/ó la *password* para entrar al sistema con permiso de sólo lectura.
- **config cli password l1 <username> [<password >]**; cambia el *login* y/ó la *password* para entrar al sistema con permiso de lectura/escritura pero sólo para cambiar los parámetros de las interfaces.
- **config cli password l2 <username> [<password >]**; cambia el *login* y/ó la *password* para entrar al sistema con permiso de lectura/escritura pero sólo con las funcionalidades de la capa 2.

- **config cli password l3 <username> [<password >]**; cambia el *login* y/ó la *password* para entrar al sistema con permiso de lectura/escritura a nivel de red (capa 3) lo cual incluye las funcionalidades de la capa 2.
- **config cli password rw <username> [<password >]**; cambia el *login* y/ó la *password* para entrar al sistema tanto con permiso de lectura como de escritura
- **config cli password rwa <username> [<password >]**; cambia el *login* y/ó la *password* para entrar al sistema con todos los permisos lectura/escritura/todos.

Nota: Para la configuración inicial del *router*, el *login* introducido será **rwa** siendo su contraseña correspondiente también **rwa** (ver figura 2.13).

PASO4: Asignar dirección *IP*.

Se debe asignar una dirección *IP* al Puerto de Gestión para poder llevar a cabo la administración y gestión del equipo a través del navegador Web, el *software* Device Manager o mediante una sesión Telnet.
Para asignar una dirección *IP* al Puerto de Gestión utilizando la *Run-Time* CLI, se debe introducir el siguiente comando:

- **config bootconfig net mgmt ip** <ipaddr/mask> **[cpu-slot-id <#>]**

donde:

- *ipaddr/mask* especifica la dirección *IP* y la máscara de subred del Puerto de Gestión.
- *cpu-slot-id #* es un parámetro opcional para especificar a qué módulo 8690FS se le asigna la dirección *IP* en caso de tener 2 módulos instalados. Si se omite, la dirección *IP* es asignada al módulo de gestión activo.

Por ejemplo, al equipo del laboratorio se le ha asignado la dirección *IP* 192.168.2.14 con máscara de red 255.255.255.0 de la siguiente forma (ver figura 2.14):

- **config bootconfig net mgmt ip 192.168.2.14/24**

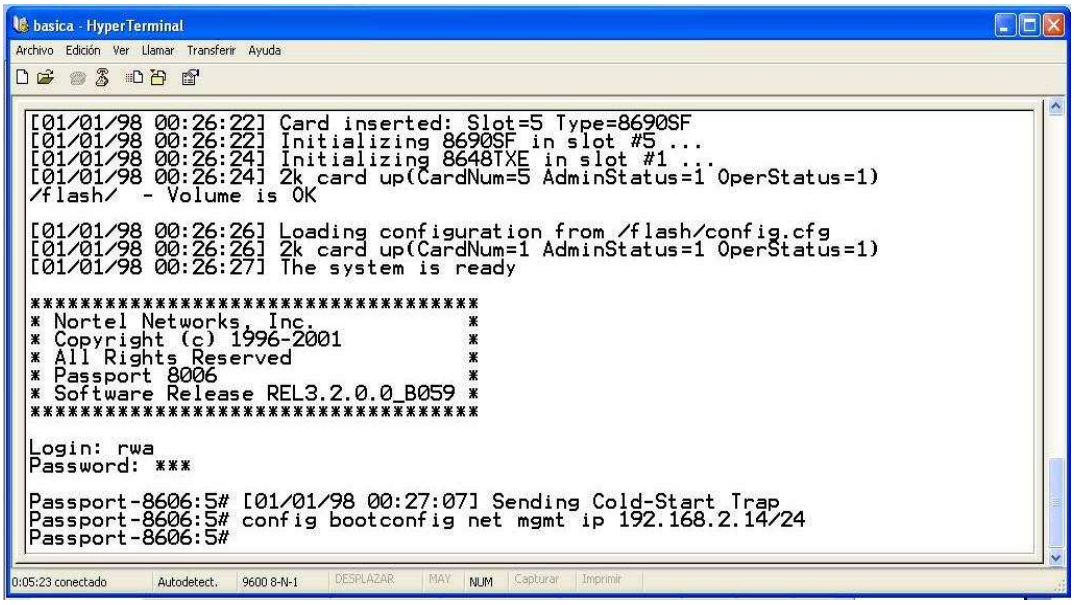


Figura 2.14: Asignación de dirección *IP* y de máscara de red al Puerto de Gestión

Una vez hecho esto, se puede comprobar los valores de la dirección *IP* y de la máscara de red asignados introduciendo el siguiente comando:

- **config bootconfig net mgmt info**

Esta instrucción muestra información de los parámetros del Puerto de Gestión, entre los que se incluyen la dirección *IP* y de la máscara de red asignados (ver figura 2.15).

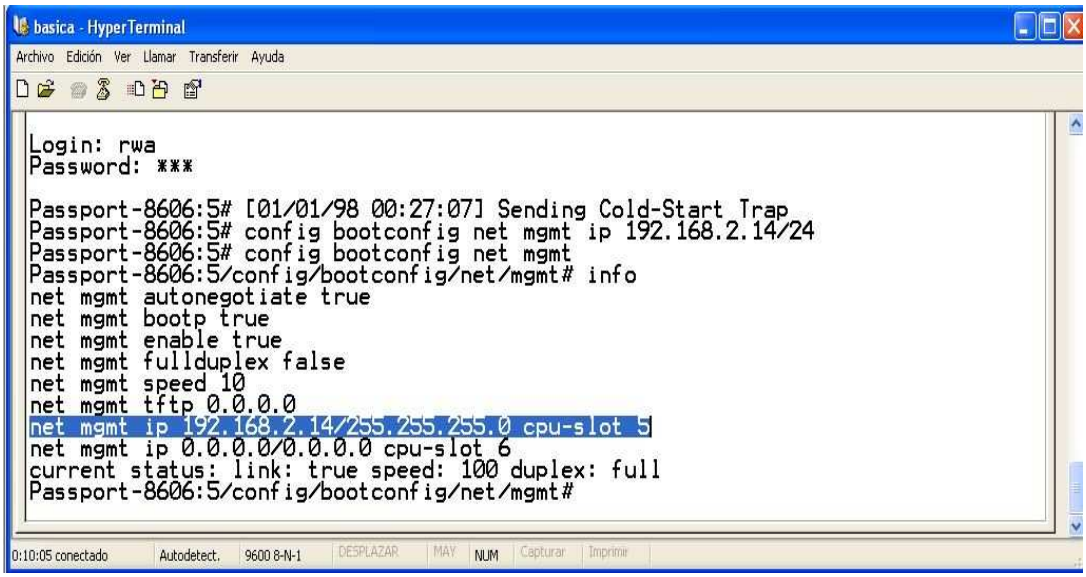


Figura 2.15: Información de estado del Puerto de Gestión

Para salvar la configuración es necesario introducir el siguiente comando antes de salir del sistema (ver figura 2.16):

- **save config**

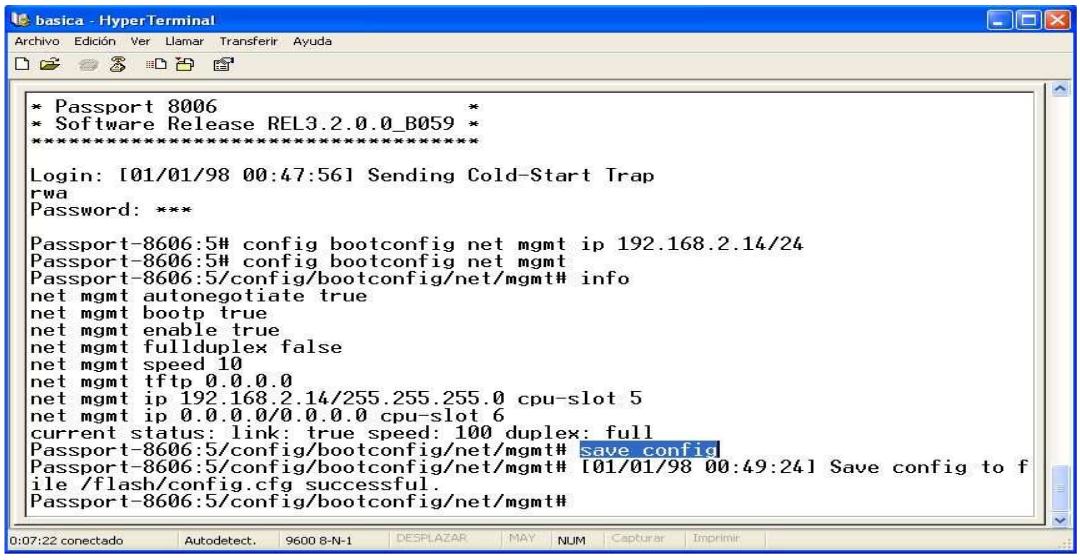


Figura 2.16: Configuración del sistema salvada satisfactoriamente

De manera equivalente, el comando que debe introducirse para la asignación de una dirección *IP* y de una máscara de red al Puerto de Gestión usando la *Boot Monitor* CLI es el siguiente (ver figura 2.17):

- **net mgmt ip** <ipaddr/mask>

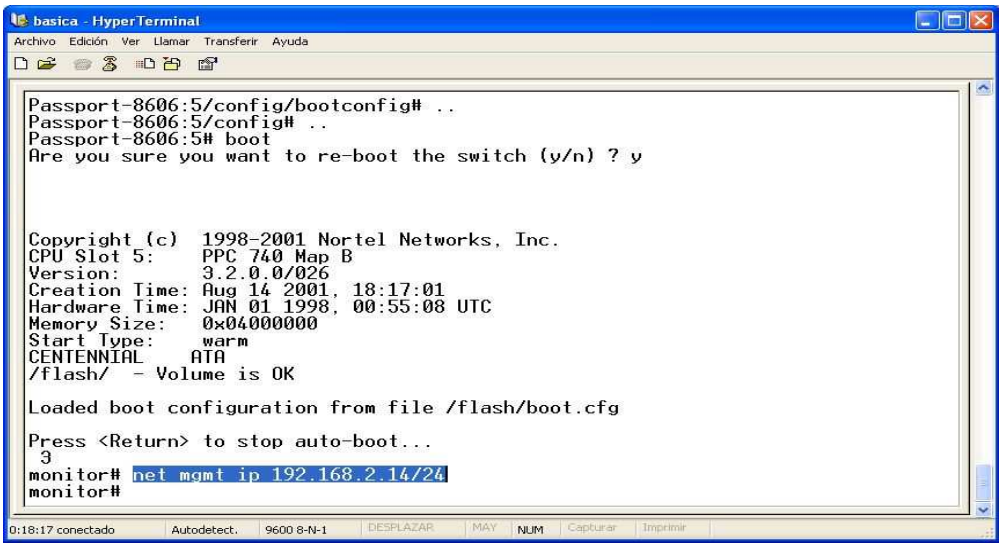


Figura 2.17: Asignación de dirección *IP* y de máscara de subred al Puerto de Gestión

Para comprobar los valores de la dirección *IP* y de la máscara de red asignados se introduce el siguiente comando:

- **net mgmt info**

Esta instrucción muestra información de los parámetros del Puerto de Gestión, entre los que se incluyen la dirección *IP* y de la máscara de red asignados (ver figura 2.18).

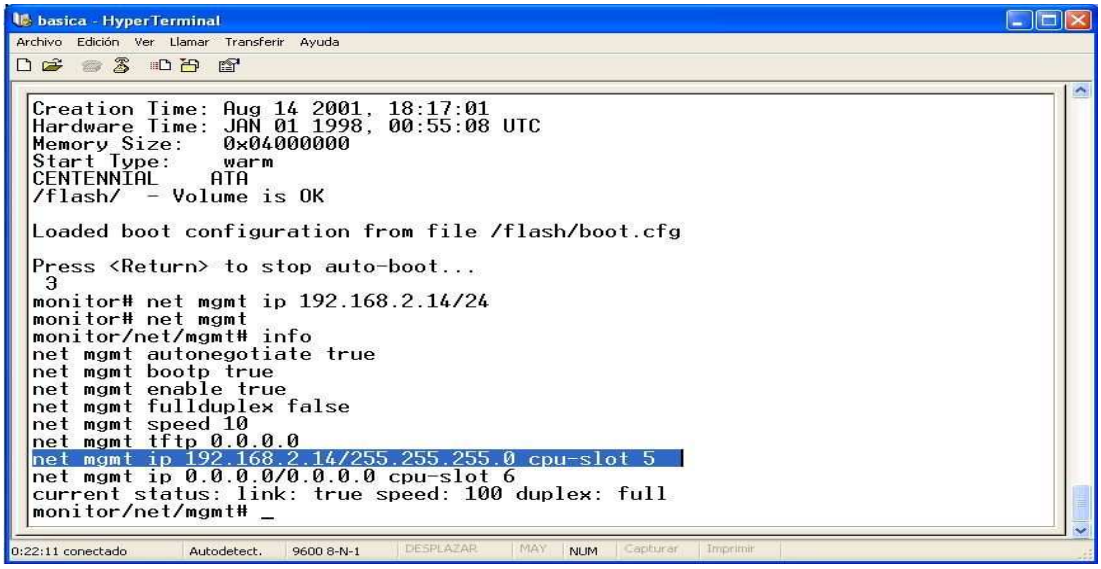


Figura 2.18: Información de estado del Puerto de Gestión

Para salvar la configuración es necesario introducir el siguiente comando antes de salir de la *Boot Monitor* CLI:

- **save**

2.2.4 Posibles Modos de Gestión y Administración del router

Una vez finalizada la configuración inicial del *router*, éste ya se puede incorporar a la red. Así que, las funciones de gestión y administración del *Passport 8600 Routing Switch*, se pueden realizar, además de a través de la CLI, utilizando el programa **Device Manager**. También, es posible visualizar la información de estado del *router* mediante un **navegador Web**.

2.2.4.1 Device Manager

La aplicación **Device Manager** es una herramienta de interfaz gráfica de usuario (GUI) basada en el protocolo SNMP (Protocolo Simple de Administración de Red, *Simple Network Management Protocol*). Este *software* permite una configuración, monitorización, administración y gestión del *router* más sencilla y cómoda que el uso de la interfaz de línea de comandos (CLI), ya que simplemente requiere ir haciendo *clic* en las opciones de la barra de Menú e introduciendo y seleccionando los parámetros necesarios de acuerdo con la tarea a realizar.

Los pasos que se deben seguir para ejecutar la aplicación son:

- Ejecutar el programa Device Manager (ver figura 2.19).

Figura 2.19: Programa Device Manager

- Seleccionar “Device > Open” ó pulsar el icono correspondiente en la barra de herramientas:

- Introducir como nombre del dispositivo su dirección *IP* (ver figura 2.20).

- Por defecto, aparecen las Comunidades, es decir, las palabras claves para la autentificación, "*Community strings*" necesarias para tener permisos de lectura y de escritura. Según SNMP el *string* correspondiente para **Read Community** es ***public***, y el *string* para **Write Community** es ***private***. Estos *strings* pueden ser modificados una vez que se haya accedido al dispositivo mediante este software.

- Open.

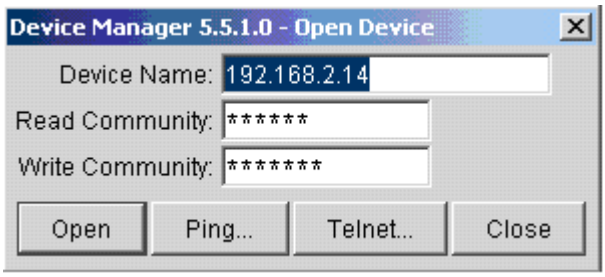


Figura 2.20: Dirección *IP* del *Passport 8600*

Una vez hecho esto, se abrirá una ventana en la que se podrá visualizar el equipo (ver figura 2.21).

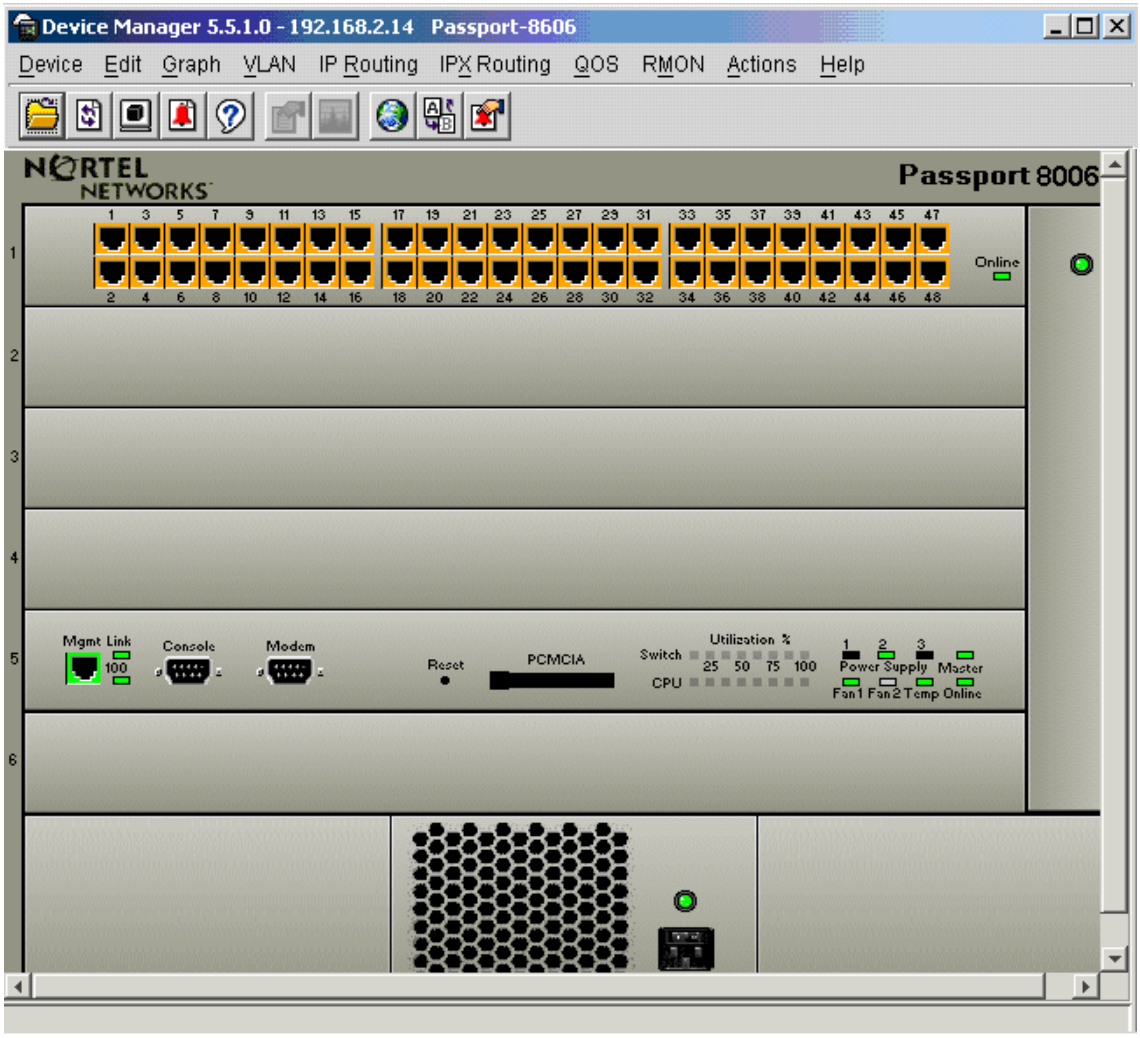


Figura 2.21: Visualización del *router Passport 8600 Routing Switch*

2.2.4.2 Navegador Web

Esta posibilidad se limita a mostrar de una manera estructurada **la información de estado** del *router Passport 8600 Routing Switch*. Es decir, que la administración a través de la interfaz Web tiene permiso de sólo-lectura (ro). Para usar esta opción, se debe introducir en un navegador Web el URL o dirección de la página Web desde la que se gestionará el *router*. El URL o dirección de la página Web se corresponde con la dirección IP que tenga asignada el *router*.

Por ejemplo, si la dirección IP que se asignó al *router* fue la 192.168.2.14, el URL correspondiente que se debe introducir será http://192.168.2.14 (ver figura 2.22):

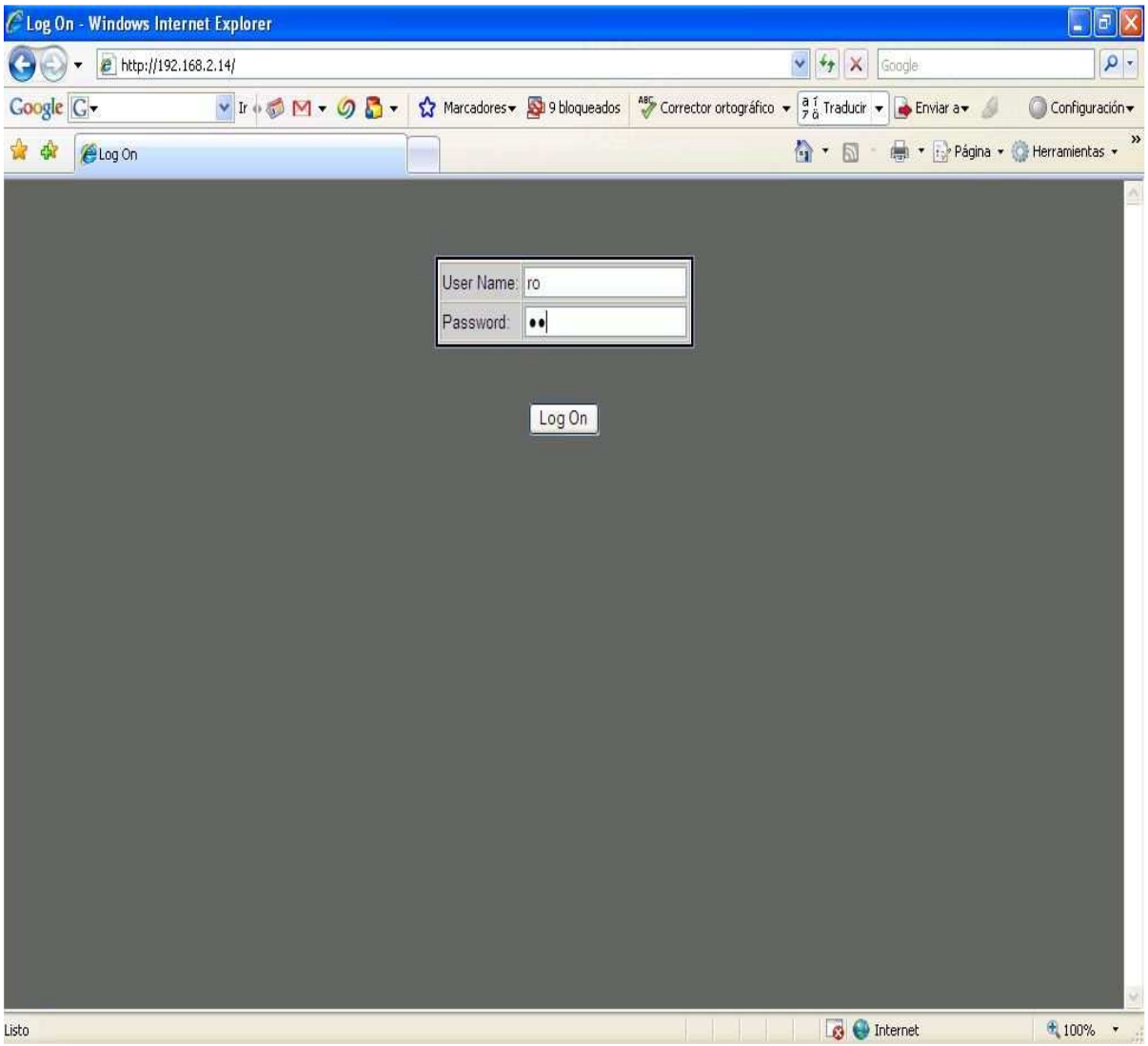


Figura 2.22: Entrada al Sistema de Gestión Web

Una vez cargada la página, antes de poder acceder al Sistema de Gestión Web, se pide un nombre de usuario (*Name User*) y un *password*.

Nota: Para poder acceder, el "*Name User*" será **ro** y su *password* correspondiente será también **ro**.

Una vez que se ha accedido a este Sistema de Gestión Web, la página Web cargada muestra de una manera estructurada **la información de estado** del *router Passport 8600 Routing Switch* (ver figura 2.23). Se pueden distinguir en la ventana, dos zonas o paneles para presentar la información. En el panel izquierdo se muestra de forma estructurada el nombre de los temas a visualizar. Para acceder a la información que se desea obtener basta con ir haciendo *clic* en los apartados correspondientes. Dicha información se visualiza en el panel derecho.

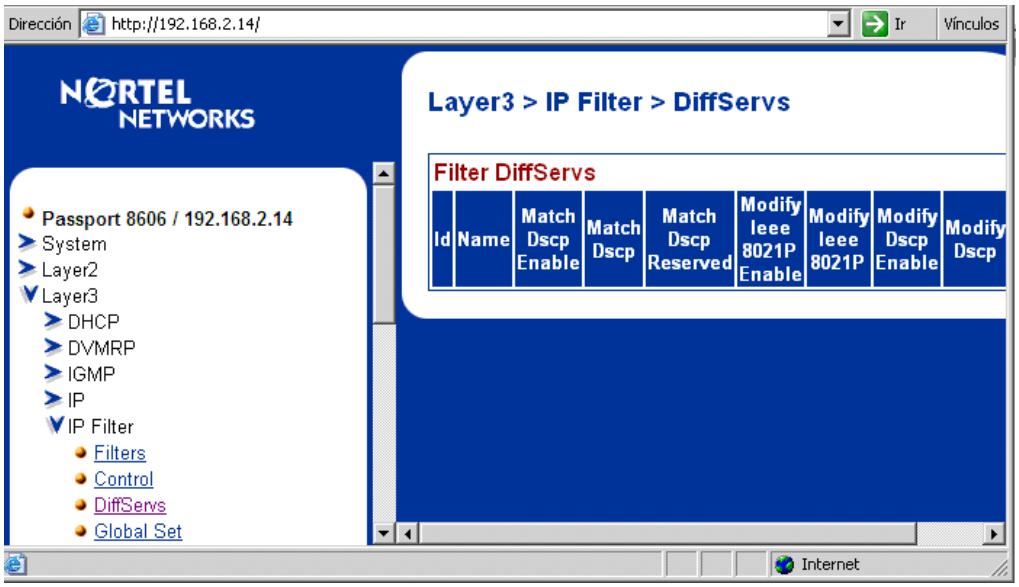


Figura 2.23: Sistema de Gestión Web del *router Passport 8600 Routing Switch*

2.3 Configuración General de los Servicios Diferenciados (DiffServ)

En este apartado, se explica cómo configurar de manera general los Servicios Diferenciados en el equipo *Passport 8600 Routing Switch* para así proveer de QoS a la red de datos. Esta configuración general incluye selección y configuración de puertos, definición de filtros y construcción de sets de filtros, definición y configuración de perfiles y políticas de descarte de paquetes.
Para la configuración, monitorización, administración y gestión de estas funciones se ha empleado la aplicación **Device Manager**, la cual es más sencilla y cómoda que el uso de la interfaz de línea de comandos (CLI), ya que simplemente requiere ir haciendo *clic* en las opciones de la barra de Menú e introduciendo y seleccionando los **parámetros** necesarios de acuerdo con la tarea a realizar para implementar *DiffServ*.

2.3.1 Pasos de la configuración

Para implementar *DiffServ* en el equipo *Passport 8600 Routing Switch* son necesarios cuatro pasos:

1. Activar el campo de *"DiffServEnable"*, seleccionar el tipo de puerto *"core/access"* y asignar una dirección IP a cada puerto perteneciente al dominio *DiffServ*.
2. Definición de filtros IP. Filtrar el tráfico para realizar la clasificación de los diferentes tipos de tráfico.
3. Construcción y aplicación de set (lista) de filtros IP a un puerto o conjunto de puertos.
4. Definición y configuración de perfiles y políticas de tráfico.

2.3.1.1 Activación del campo *"DiffServEnable"*, selección del tipo de puerto *"core/access"* y asignación de dirección IP

En primer lugar, hay que activar el campo *"DiffServEnable"* en los puertos que van a formar parte del dominio *DiffServ*, y seleccionar el tipo de puerto *"core/access"* dependiendo de cuáles sean las acciones de QoS que éstos van a aplicar sobre su tráfico entrante y saliente. Además, se les asignará a cada uno de estos puertos una dirección IP.

Para acceder a estos parámetros, se edita el puerto en cuestión. Para editar un puerto, se puede hacer doble-*clic* sobre el puerto, o bien, se puede seleccionar dicho puerto y elegir desde la barra de menú de Device Manager **Edit > Port**, o bien, desde la barra de herramientas del Device Manager se pulsa el botón de edición:

Entre todas sus etiquetas, la **etiqueta "Interface"** se abre por defecto, y es donde se establece y comprueba la configuración básica del puerto. En ella es donde se activa el campo "*DiffServEnable*" y se selecciona el tipo de puerto *"core/access"*. (Ver figura 2.24).

Figura 2.24: Activación del campo "*DiffServEnable*" y selección del tipo de puerto *"core/access"*

En la **etiqueta "IP Address"** es donde se le asigna una dirección IP al puerto en cuestión. (Ver figura 2.25).

Figura 2.25: Asignación de dirección IP a un puerto

Se selecciona el **botón "Insert"** y se rellenan el campo *"Ip Address"* para la dirección IP y el campo *"Net Mask"* para la máscara de subred del puerto.

2.3.1.1.1 Funciones de los puertos "core/access" y Clases de QoS en Nortel

Los puertos de entrada y salida a un **dominio *DiffServ*** a los que llegan y salen sus respectivos flujos de tráfico se configuran como nodos frontera (***access port***), y los puertos en el interior de la red *DiffServ* se configuran como nodos interiores (***core port***). Toda la complejidad de este esquema se traslada a la frontera de la red, manteniendo el interior tan simple como sea posible. Es en los extremos de la red, en los puertos *access*, donde se llevan a cabo todas las **funciones necesarias para implementar *DiffServ*:**

- Tiene lugar el **acondicionamiento del tráfico** mediante funciones policía (*Traffic Policing)*, con *Token Buckets*, comprobando si los flujos de tráfico cumplen sus contratos.

- El **marcado DSCP**. Los paquetes que cumplan el contrato serán marcados con un determinado valor DSCP y aquellos cuya tasa supere lo contratado se marcarán con un DSCP distinto.

- La **clasificación de los paquetes**. El tráfico se divide y se identifica dentro de **Clases de Servicio**. Cada paquete sale de un puerto *access* con un valor DSCP o bits IEEE 802.1p que se corresponden con un nivel de QoS. Los puertos *core* simplemente manejan los paquetes basándose en el marcado establecido por los puertos *access*, es decir, aceptan todos los **mapeos previos** realizados en los puertos *access* y colocan los paquetes en **la cola correcta** de QoS basándose en su valor de marcado DSCP.

La figura 2.26 ilustra una implementación típica de puertos *core* y *access* en un dominio *DiffServ*.

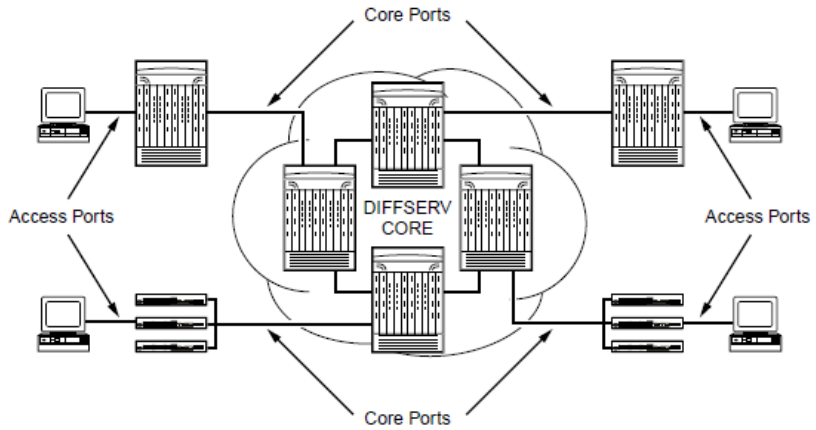


Figura 2.26: Implementación de puertos *core* y *access* en un dominio *DiffServ*

Para la **identificación** de los **diferentes agregados de tráfico**, **Clases de Servicio** a las que pertenece cada paquete, se define un código llamado **DSCP** (*DiffServ CodePoint*). Este código está formado por los seis bits más significativos del campo DS (*DiffServ*) de la cabecera de los paquetes IP. El campo DS tiene un tamaño de 1 byte. El campo DS renombra al campo **ToS** (*Type of Service*) en el caso de utilizar IPv4, y al campo ***Traffic Class*** cuando usemos IPv6. Los dos bits menos significativos del campo DS no están en uso actualmente y su valor es ignorado por los nodos que implementan *DiffServ*. Estos dos bits están bajo experimentación en redes ECN (*Explicit Congestion Notification*) para notificar cuando hay congestión en la red.

Así pues, mediante el código DSCP, los *routers* pertenecientes al dominio *DiffServ* pueden aplicar el tratamiento correspondiente a cada paquete, es lo que se conoce como **Comportamiento por Salto** (PHB, *Per-Hop Behaviour*). Para cada Clase de tráfico se define un comportamiento por salto PHB, un **conjunto de reglas** para el tratamiento del tráfico. La aplicación de estos **perfiles de comportamiento** en todos los nodos del dominio *DiffServ* permitirá que los diferentes agregados **reciban más o menos recursos** según como hayan sido etiquetados. El **PHB asigna un nivel de prioridad** a cada clase de tráfico, que indica qué flujos tienen **mayor precedencia** frente a otros flujos que pertenezcan a clases de tráfico con menor nivel de prioridad.
En el modelo *DiffServ* existen tres perfiles PHB definidos: *Expedited Forwarding* (EF), *Assured Forwarding* (AF) y *Best-Effort* (BE).

En la tabla 2.2 se muestra el mapeo entre los valores DSCP, los bits IEEE 802.1p, el nivel de QoS y las **Clases de Servicio** que recibe el tráfico.

Tabla 2.2: Mapeo entre DSCP, bits IEEE 802.1p, nivel de QoS y Clase de Servicio

DSCP*	IEEE 802.1p	QoS Level	Traffic Service Class
CS7 (111000), CS6 (110000)	7	7	Network
EF (101110), CS5 (101000)	7	6	Premium
AF41 (100010), AF42 (100100), AF43 (100110), CS4 (100000)	6	5	Platinum
AF31 (011010), AF32 (011100), AF33 (011110), CS3 (011000)	5	4	Gold
AF21 (010010), AF22 (010100), AF23 (010110), CS2 (010000)	4	3	Silver
AF11 (001010), AF12 (001100), AF13 (001110), CS1 (001000)	3	2	Bronze
DE (000000) and all undefined codepoints	0	1	Standard
User-defined codepoints	2	0	Standby

* The DSCP está representado en los formatos de los dos grupos PHB (AF = *Assured Forwarding*; EF = *Expedited Forwarding*; CS = *Class Selector*) y en el equivalente formato binario.

El *Passport 8600 Routing Switch* soporta las siguientes **Clases de QoS** Nortel Networks:

a. **Network**. Estas clases tienen la mayor prioridad sobre el resto del tráfico.

b. **Premium**. Es un servicio end-to-end (extremo a extremo) funcionando similar a una línea dedicada. El tráfico en esta clase de servicio está garantizado. Se trata de aquellos flujos de tráfico que **requieran** pocas pérdidas, ancho de banda mínimo asegurado, así como un retardo limitado y una variación de retardo máxima determinada (el agregado no ve colas o ve colas muy pequeñas). Adecuado para aplicaciones de tiempo real como vídeo y voz sobre IP. El PHB recomendado para este servicio es el *Expedited Forwarding* EF-PHB (Tránsito expedito). Este servicio es también conocido como **"servicio superior"**, es el mejor servicio que la red puede ofrecer. El perfil EF- PHB está identificado por el código DSCP: **101110**.

c. **Platinium, Gold, Silver y Bronze**. Estas clases usan el Servicio Asegurado AF-PHB (*Assured Forwarding*). Garantiza un caudal mínimo al usuario final, normalmente la velocidad contratada, y si existe ancho de banda no contratado permitir a los usuarios finales consumirlo. Se utilizan para tiempo real, tráfico tolerante al retardo y que no es en tiempo real y para tráfico de misión crítica. No es posible indicar requisitos temporales para estos flujos (retardo/jitter).
El perfil AF-PHB define **cuatro tipos de clases diferentes**: Bronce, Plata, Oro y Platino, en función de los **recursos reservados para las mismas**. Dentro de cada clase se establecen **tres prioridades de descarte de paquetes** (tres valores *drop-precedence*). De forma que el perfil AF define un conjunto de **12 posibles servicios**. Si identificamos cada servicio con dos subíndices AFxy, donde la variable "***x***" representaría la clase, mientras que la variable "***y***" identificaría la prioridad de descarte (alta, media y baja). Este perfil resulta muy adecuado para la implementación de los **servicios olímpicos**, donde se puede asignar a cada agregado de tráfico la clasificación de oro, plata o bronce, de forma que reciba los recursos correspondientes en cada nodo que atraviese por el dominio DiffServ. El perfil AF-PHB correspondiente se identifica mediante los códigos DSCP codificados de la siguiente manera:

- **Valor DSCP = 'cccdd0'**

  - **ccc = clase**
  - **dd = descarte**; probabilidad de descarte (*drop-precedence*).

Con este sistema, un dispositivo da la **prioridad** al tráfico por **la clase primero**. **Después** distingue y da la prioridad al tráfico **de la misma clase** tomando la **probabilidad de descarte (***drop-precedence*). (Ver tabla 2.3)

Tabla 2.3: Servicios Olímpicos y Probabilidad de Descarte

Drop	Clase 1 Bronce	Clase 2 Plata	Clase 3 Oro	Clase 4 Platino
Bajo **'01'**	001010 AF11 DSCP 10	010010 AF21 DSCP 18	011010 AF31 DSCP 26	100010 AF41 DSCP 34
Medio **'10'**	001100 AF12 DSCP 12	010100 AF 22 DSCP 20	011100 AF32 DSCP 28	100100 AF42 DSCP 36
Alto **'11'**	001110 AF13 DSCP 14	010110 AF23 DSCP 22	011110 AF33 DSCP 30	100110 AF43 DSCP 38

Menor probabilidad de descarte

Mayor probabilidad de descarte

Menor prioridad — **Mayor prioridad**

d. **Standard**. Es el servicio IP *best-effort*.

Un puerto *access*, siempre modifica (marca) el valor DSCP del paquete, antes de que el paquete sea enviado a la red. Los paquetes llegan y se clasifican en una determinada Clase de servicio. A continuación, son marcados con su correspondiente valor DSCP. Y por último, son colocados en la cola correspondiente a su nivel de prioridad para ser servidos.
La figura 2.27 ilustra cómo varias clases de paquetes son procesados a través de un puerto *access*.

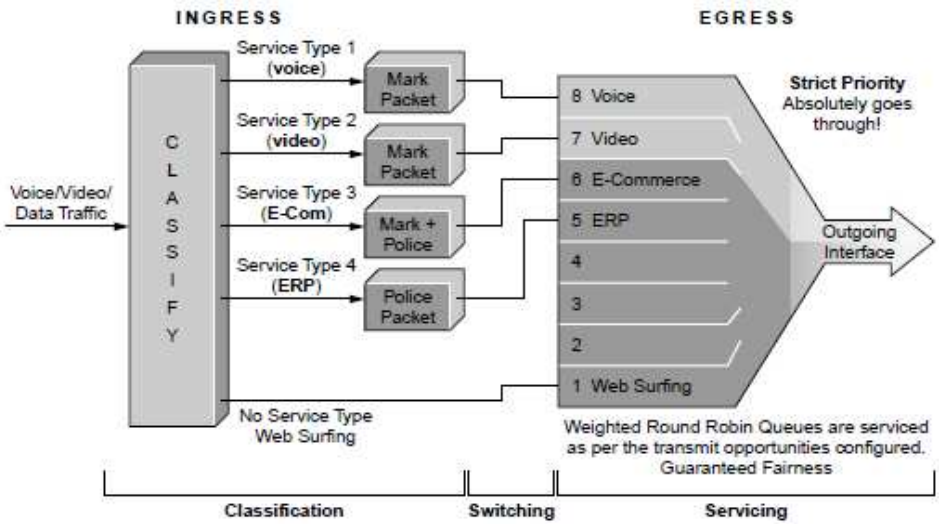


Figura 2.27: Puerto tipo *access* en el *Passport 8600*

Por ejemplo, el tráfico de voz y vídeo (sensible al retardo) es marcado con un valor DSCP para recibir la más alta prioridad, es colocado en las colas 8 y 7 de más alta prioridad. A medida que los paquetes atraviesan la red *DiffServ*, estos flujos de voz y vídeo se reenviarán antes que cualquier otro tipo de tráfico, como puede ser el tráfico *Web Surfing*, el cual es colocado en la cola 1 de más baja prioridad ya que este tráfico es tolerante al retardo. La arquitectura *DiffServ* realiza la discriminación de servicios entre los distintos flujos de tráfico ofreciendo los recursos de la red a **las clases de servicio** más altas a expensas de las clases de servicio más bajas.

Los puertos *core* confían en el marcado de QoS de los paquetes entrantes y pasan los paquetes a través de la red basándose en sus valores DSCP y los bits IEEE 802.1p. Un *core port* no permite el remarcado DSCP porque asume que el marcado DSCP se hizo antes de la entrada al puerto. Un puerto *core* no cambia la clasificación ni el marcado realizados en el puerto *access*. El puerto *core* conserva el marcado DSCP o los bits IEEE 802.1p de todos los paquetes entrantes y usa estas marcas para asignar el paquete a una cola interna.
La figura 2.28 ilustra cómo varias clases de paquetes son procesados a través de un puerto *core*.

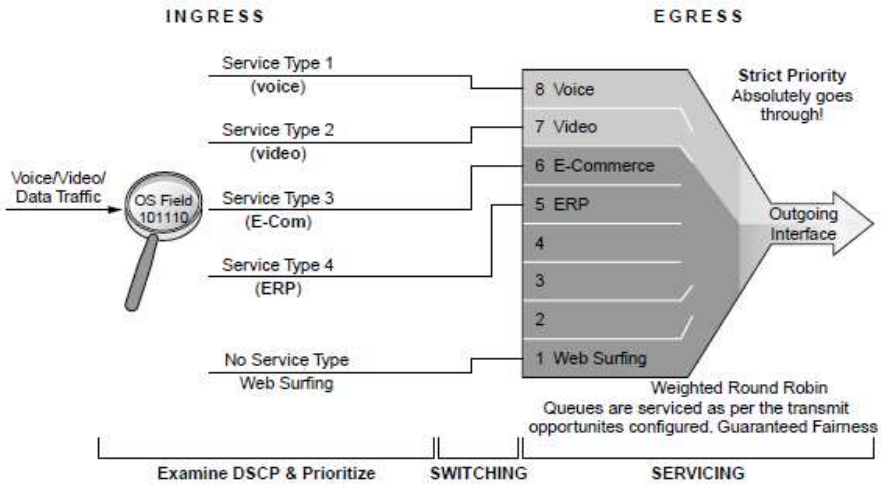


Figura 2.28: Puerto tipo *core* en el *Passport 8600*

2.3.1.2 Definición de Filtros IP

Los filtros de tráfico permiten establecer criterios para la identificación de un microflujo o un agregado de flujos, mediante la **coincidencia de múltiples campos de la cabecera de un paquete IP**.

El filtrado IP (*IP Filtering*) se usa para gestionar y procesar el tráfico global entrante al router y de este modo **clasificarlo** en los distintos tipos de tráfico. Los filtros se aplican a un puerto mediante los *"filter sets"* (listas de filtros). Cada filtro forma parte de una lista de filtros (***filter set***) que se aplica a un puerto o conjunto de puertos determinado. Cada *"filter set"* registra un surtido de criterios de coincidencia definidos y unas **acciones especificadas** (reenvío, descarte, *mirror*, priorizar, stop-on-match) a ejecutar cuando **alguno de esos criterios de filtrado se satisface.** Los paquetes que coincidan con las condiciones de filtrado, siguen la acción especificada en el filtro.
Los **contadores** de filtros se mantienen para todos los **filtros activos**. Cada vez que un **filtro activo** tiene un acierto "hit" por un **paquete**, su contador se incrementa en uno. El administrador puede visualizar y resetear en cualquier momento estos contadores.

Los filtros IP se aplican a los puertos de entrada del conmutador con una **acción por defecto** para reenviar o descartar los paquetes. Todos los paquetes que no coincidan con ninguna condición de filtrado de un puerto son **reenviados o descartados** en función de la **acción por defecto del puerto**. Las acciones de filtros individuales pueden sobrescribir las acciones por defecto del puerto.

Se pueden aplicar dos tipos de filtros: los **filtros de tráfico** y los **filtros globales**.

a) **Filtros globales:** se ejecutan en un componente hardware llamado **ARU** (*Address Resolution Unit*, Unidad de Resolución de Direcciones). Este ARU es un ASIC (circuito integrado de propósito específico) que **realiza la decisión de** encaminamiento sin requerir la actividad de la CPU, y por tanto, se consiguen grandes velocidades de **reenvío**.
   Se pueden configurar hasta un máximo de ocho filtros globales por grupo de ocho puertos 10BASE-T/100BASE-T o por puerto Gigabit Ethernet. Estos filtros se pueden aplicar a tráfico IP bridged y a tráfico IP routed si no se realizan operaciones *DiffServ*. Por tanto, los filtros globales sólo se pueden aplicar sobre los **puertos *access DiffServ*** si el tráfico es IP bridged.
   Los **filtros globales** pueden especificar una dirección IP origen y su máscara de subred, una dirección IP destino y su máscara de subred, ambas o ninguna de ellas. No existe una longitud mínima o máxima de la máscara de subred.

b) **Filtros origen/destino:** se almacenan en la memoria asociados con la ARU. El tiempo requerido para ejecutar una decisión de encaminamiento de un paquete depende del número de filtros origen/destino configurados y asociados con las direcciones IP origen/destino de este paquete. Por tanto, Nortel recomienda, para **minimizar el tiempo de búsqueda** necesario para completar una decisión de encaminamiento, reducir el número de filtros origen/destino asociados con una dirección IP, diseñar los filtros origen/destino lo más específicos como sea posible y usar máscaras de subred de longitud lo máxima posible, para evitar búsquedas entre cuantiosos filtros asociados a diferentes flujos de tráfico IP.
   Son los llamados "filtros de tráfico" y dan las órdenes a las interfaces del router para manejar selectivamente el tráfico IP especificado. Se determina qué paquetes reciben un tratamiento especial basándose en el valor de uno o más campos de la cabecera de los paquetes (dirección origen, dirección destino, número de puertos de origen y de destino, el campo DS, etc). Mediante los "filtros de tráfico" se puede reducir **la congestión** en la red y controlar el acceso a los recursos de la red mediante bloqueo, reenvío, o dando prioridad a tráfico especificado sobre una interfaz. Se pueden aplicar múltiples "filtros de tráfico" a una única interfaz.
   Los **filtros origen** deben especificar una dirección IP origen y su máscara de subred, y opcionalmente puede especificar una dirección IP destino y su máscara de subred. Los **filtros destino** deben especificar una dirección IP destino y su máscara de subred, y opcionalmente puede especificar una dirección IP origen y su máscara de subred. La longitud mínima de la máscara de subred es de ocho bits.

Los identificadores IDs de filtro van desde el 1 hasta el 4096. Los identificadores del 3072 hasta el 4096 están reservados para uso interno del sistema (filtros del sistema), por lo que no se deben usar. Se pueden configurar hasta 3071 filtros, entre todos los puertos o sobre un único puerto, incluyendo filtros origen/destino y filtros globales.

Los criterios de coincidencia para los filtros en los conmutadores *Passport* pueden ser cualquiera de los siguientes:

- Dirección destino o rango de direcciones.
- Dirección origen o rango de direcciones.
- Requerir que coincida un protocolo IP (TCP, UDP o ICMP).
- Número de puertos TCP o UDP.
- Conexiones TCP establecidas solamente dentro de la red o establecimiento bidireccional permitido.
- Petición ICMP.
- Campo DS.
- Fragmento trama IP.

Un filtro origen/destino o global puede causar las siguientes **acciones** para ser ejecutadas sobre **un paquete** que coincida con los **criterios de selección del filtro**:

- Reenviar el paquete cuando el filtro se aplica con un modo de acción de reenvío (*Forward*).
- Descartar el paquete cuando el filtro se aplica con un modo de acción de descarte (*Drop*).
- Reflejar el paquete hacia el 'puerto *mirror*' definido.
- Función de Policía (*Policing*).
- Conexión TCP (evita sesiones TCP entrantes).
- Stop on match.
- Igualar el campo DS.
- Modificar el código DSCP (sólo en los 'puertos *access*' *DiffServ*).
- Modificar los bits IEEE 802.1p.

Las acciones dependen del modo de acción del puerto y del modo de acción del filtro. Cuando se define un filtro, se selecciona el **'Modo'** de acción del filtro: ***"UseDefaultAction"***, ***"Forward"***, ***"Drop"***, ***"ForwardToNextHop"***. En la tabla 2.4 se muestra la acción que se lleva a cabo según se seleccione un modo u otro en el filtro y cual sea la acción por defecto del puerto.

Tabla 2.4: "Modos de acción" de un filtro

Puerto	Modo del Filtro	Acción sobre el paquete
Reenvío (forward)	Default	Se reenvían todos los paquetes que coincidan
Descarte (drop)	Default	Se descartan todos los paquetes
Reenvío (forward)	Reenvío (forward)	Se reenvían todos los paquetes que coincidan
Descarte (drop)	Reenvío (forward)	Se descartan todos los paquetes excepto los que coincidan con el filtro
Reenvío (forward)	Descarte (drop)	Se descartan todos los paquetes que coincidan con el filtro
Descarte (drop)	Descarte (drop)	Se descartan todos los paquetes

Cada filtro tiene un **modo de acción** asociado, el cual determina si los paquetes que coincidan con este filtro son reenviados (forward) a través del conmutador o son descartados (drop).
Cada puerto filtrado en el conmutador *Passport 8600* tiene una acción por defecto asociada de reenvío o de descarte. Cuando el modo de la acción de filtrado coincide con la acción por defecto del puerto, se toma la **acción por defecto del puerto**.

Cuando la acción por defecto del puerto es de descarte, un paquete sólo se reenvía si una coincidencia del filtro se estableció con un modo de acción de reenvío. Si ocurre una única coincidencia con un modo de acción de reenvío, no importa cuántas coincidencias de filtros se dan con un modo de acción de descarte; **la trama se reenvía**. Es decir, si un paquete coincide con múltiples filtros y cualquiera de ellos tiene un modo de acción de reenvío, el paquete es reenviado.
Cuando el modo de acción del puerto es de reenvío, un paquete se descarta sólo si una coincidencia del filtro se estableció con un modo de acción de descarte. De nuevo, si ocurre una única coincidencia con un modo de acción de descarte, no importa cuántas coincidencias de filtros se dan con un modo de acción de reenvío; **la trama se descarta**. Es decir, si un paquete coincide con múltiples filtros y cualquiera de ellos tiene un modo de acción de descarte, el paquete es descartado.

Para insertar un filtro IP, desde la barra de menú de Device Manager se selecciona **IP Routing > Filter**. La **etiqueta "Filters"** se abre por defecto, y en ella se visualiza la información básica de los filtros añadidos. (Ver figura 2.29).

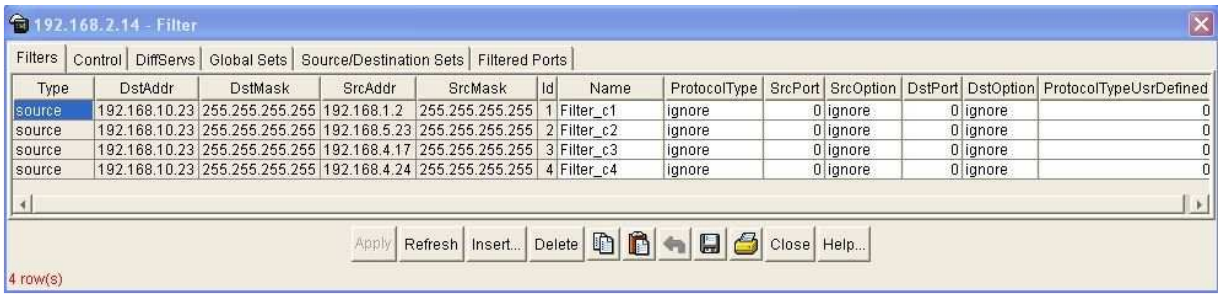


Figura 2.29: Etiqueta "Filters". Información básica de los filtros añadidos.

Para definir **la plantilla de un nuevo filtro** (ver figura 2.30) **a insertar** se hace clic sobre el botón **"Insert"**:

- Se selecciona el **'Tipo'** de filtro: **filtro global** ó **filtro de tráfico origen/destino**. Seguidamente, aparecen los campos para establecer las "condiciones de filtrado". La descripción de estos campos se muestra en la tabla 2.5.

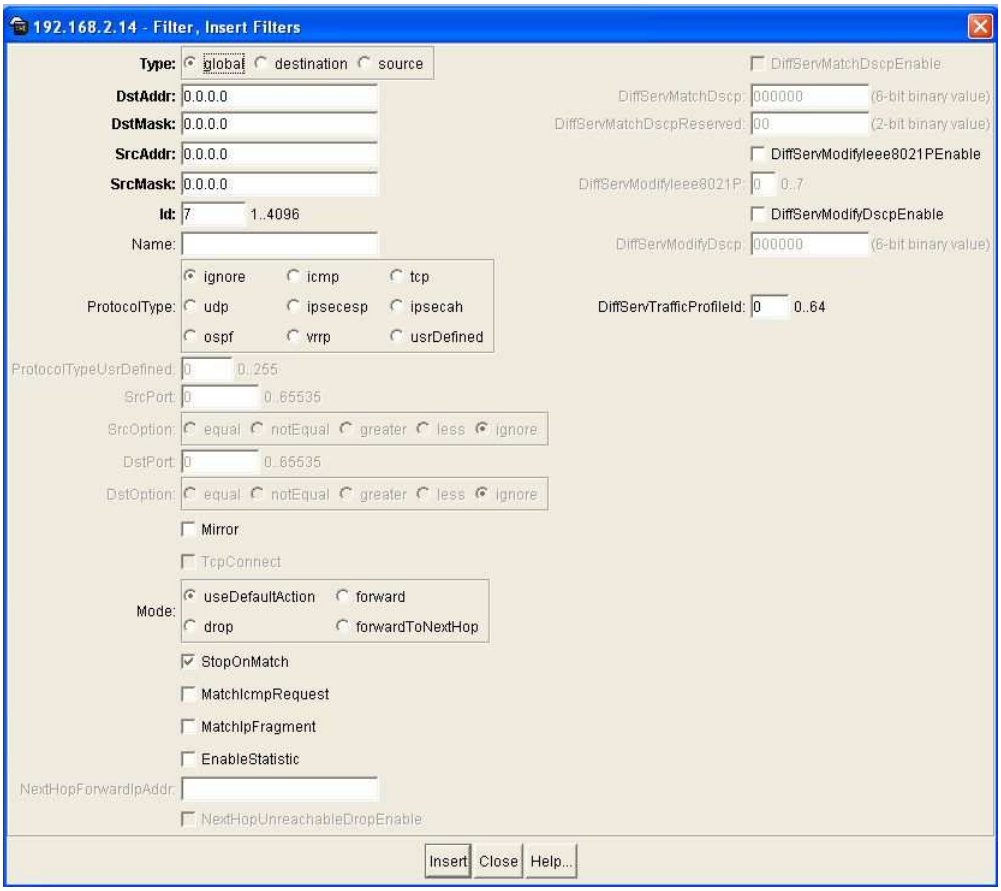


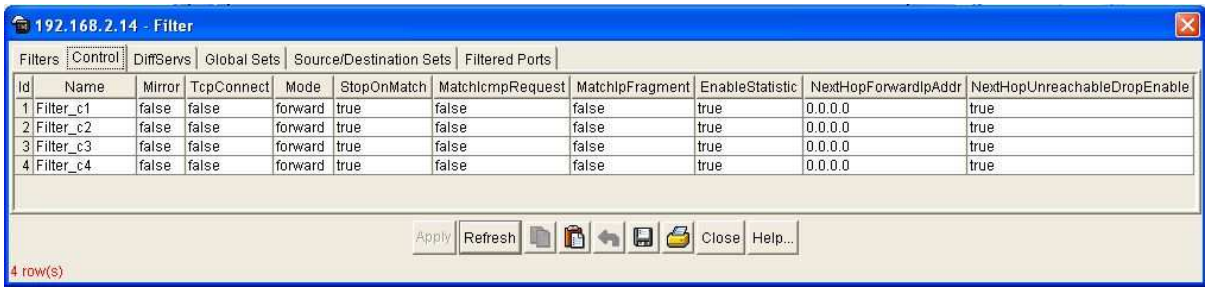
Figura 2.30: Plantilla de configuración de un filtro

Tabla 2.5: Descripción de los campos de la plantilla de un filtro

Campo	Descripción
Type	El tipo del filtro: • Global • Destination • Source Nota: El establecido por defecto es Global.
DstAddr	Dirección IP destino.
DstMask	Máscara de subred destino.
SrcAddr	Dirección IP origen.
SrcMask	Máscara de subred origen.
Id	El ID del filtro (1 a 4096)
Name	El nombre del filtro IP.
ProtocolType	El tipo de protocolo IP (ignore, icmp, tcp, udp) Nota: Se establece por defecto a ignore.
SrcPort	El número de puerto origen TCP/UDP.
SrcOption	La opción de puerto origen TCP/UDP (equal, not equal, greater, less, ignore) Nota: Se establece por defecto a ignore.
DstPort	El número de puerto destino TCP/UDP.

DstOption	La opción de puerto destino TCP/UDP (equal, not equal, greater, less, ignore) Nota: Se establece por defecto a ignore.
Mirror	Permite reflejar el paquete al puerto mirror definido.
TcpConnect (sólo tcp)	Se activa para permitir sólo las conexiones TCP establecidas dentro de la red o se desactiva para permitir establecimiento bidireccional.
Mode	Se opta entre los tres modos de acción del filtro: *useDefaultAction*, *forward*, *drop* o *dropforwardToNextHop*.
StopOnMatch	Hace que el filtro se detenga en las coincidencias definidas en el filtro, es decir, las coincidencias de los múltiples campos de cada paquete IP. Activado por defecto.
MatchIcmpRequest	Se activa si se desea que las coincidencias sobre los paquetes de petición ICMP sean ejecutadas.
MatchIpFragment	Se activa si se desea que las coincidencias sobre los fragmentos de los paquetes IP sean ejecutadas.
EnableStatistic	Se activa si se desean estadísticas para este filtro.
NextHopForwardIpAddr (sólo filtro origen/destino)	Se establece para aplicar el filtro al siguiente salto.
NextHopUnreachableDropEnable (sólo filtro origen/destino)	Se activa si se desea acción de descarte.
DiffServMatchDscpEnable (sólo filtro origen/destino)	Se activa para permitir coincidencias con el campo DS (8 bits), el cual se compone de los 6-bits DS codepoint (DSCP) y de los 2-bits de reserva.
DiffServMatchDscp	En este campo se especifica el valor DSCP. El usuario debe introducir un valor binario de 6 bits, y por defecto, este valor es 000000. Si el DSCP de los paquetes entrantes coincide con este valor, entonces este filtro se aplica sobre el paquete.
DiffServMatchDscpReserved	Este campo se reserva para uso futuro. Por defecto el valor binario para los 2 bits es 00 y no debería ser cambiado.
DiffServModifyIeee8021PEnable	Se activa para permitir que el campo IEEE 802.1p sea modificado solamente en los paquetes entrantes a los puertos DiffServ access. Por defecto, el campo IEEE 802.1p se establece a cero.
DiffServModifyIeee8021P	Si no se quiere establecer el campo IEEE 802.1p a cero, se usa este campo para especificar el valor del campo IEEE 802.1p. Antes de introducir el valor, se establece el campo Modifyleee8021PEnable a “false”, y después de introducirlo hay que establecerlo a “true”.
DiffServModifyDscpEnable	Se activa para permitir que el DSCP (6 bits) sea modificado solamente en los paquetes entrantes a los puertos DiffServ access. Por defecto, el DS codepoint se establece a 000000.
DiffServModifyDscp	Si no se quiere establecer el DSCP a cero, se usa este campo para especificar el valor del DSCP. Antes de introducir el valor de 6 bits, se establece el campo ModifyDscpEnable a “false”, y después de introducirlo hay que establecerlo a “true”.
DiffServTrafficProfileId	Este campo se usa para especificar qué perfil de tráfico debe ser aplicado a los paquetes que coincidan con este filtro. Un valor de cero significa que no se aplica ningún perfil de tráfico.

El conjunto de todos estos campos, se distribuye en: información básica del filtro en la etiqueta **“Filters”**, información de control en la etiqueta **“Control”** e información de filtrado *DiffServ* en la etiqueta **“DiffServs”**. Esta información se puede editar y cambiar a un nuevo valor haciendo clic en los campos con el fondo blanco. Para salvar los nuevos valores se hace clic en “Apply” y después en “Refresh”. Una vez hecho esto, se debe volver a aplicar los puertos asociados con el filtro en cuestión.
En la figura 2.31 se puede visualizar y manejar **información de control** de los filtros insertados.

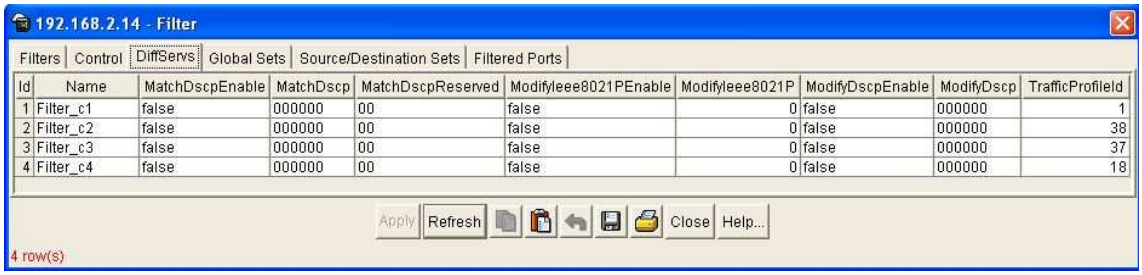


Id	Name	Mirror	TcpConnect	Mode	StopOnMatch	MatchIcmpRequest	MatchIpFragment	EnableStatistic	NextHopForwardIpAddr	NextHopUnreachableDropEnable
1	Filter_c1	false	false	forward	true	false	false	true	0.0.0.0	true
2	Filter_c2	false	false	forward	true	false	false	true	0.0.0.0	true
3	Filter_c3	false	false	forward	true	false	false	true	0.0.0.0	true
4	Filter_c4	false	false	forward	true	false	false	true	0.0.0.0	true

Figura 2.31: Etiqueta "Control". Información de Control de los filtros añadidos.

Por ejemplo, el filtro de identificador Id=1, se ha nombrado "Filter_c1", su modo de acción es reenviar (forward) los paquetes que coincidan con los criterios de selección, se van a recoger estadísticas de los paquetes y se activa la posibilidad de que haya descarte de paquetes.

La siguiente **etiqueta** es **"DiffServs"** y en ella se establecen los parámetros de los Servicios Diferenciados. (Ver figura 2.32).



Id	Name	MatchDscpEnable	MatchDscp	MatchDscpReserved	Modifyleee8021PEnable	Modifyleee8021P	ModifyDscpEnable	ModifyDscp	TrafficProfileId
1	Filter_c1	false	000000	00	false	0	false	000000	1
2	Filter_c2	false	000000	00	false	0	false	000000	38
3	Filter_c3	false	000000	00	false	0	false	000000	37
4	Filter_c4	false	000000	00	false	0	false	000000	18

Figura 2.32: Etiqueta "DiffServs". Información de los Servicios Diferenciados.

Por ejemplo, a los paquetes que coinciden con los criterios del filtro Filter_c3 se les aplica el Perfil de tráfico con identificador número 37. El resto de campos están desactivados ya que los paquetes que llegan a los puertos *access* asociados a este filtro aún no han sido marcados con ningún valor DSCP.

2.3.1.3 Construcción de Sets de Filtros IP y aplicación a un puerto o conjunto de puertos.

Como ya se ha mencionado, un filtro o un conjunto de filtros pertenecen a un ***Filter Set*** el cual registra unas acciones que se aplican sobre un puerto o un conjunto de puertos.
Una colección de **filtros origen/destino** se define en un set de filtros **origen/destino**, y el set es aplicado a un puerto o grupo de puertos. Se pueden asignar múltiples sets a cualquier puerto dado.
Una colección de **filtros globales** se define en un set de filtros global (no excediendo ocho por set), y el set es aplicado a un puerto o grupo de puertos. Se pueden asignar múltiples sets a un puerto dado o a un grupo de puertos, pero el máximo número de filtros globales que se pueden activar sobre un puerto dado es de ocho.
En los siguientes apartados, se explica cómo crear un **set de filtros global** y cómo crear un **set de filtros origen/destino**.

2.3.1.3.1 Construcción de Sets de Filtros Globales

Se debe tener en cuenta que hasta un máximo de ocho filtros globales se pueden aplicar sobre cualquier set de puertos RaptARU. Un set incluye ocho puertos 10/100 Mbps o un puerto de 1 Gbps, cada uno de los cuales puede contener hasta ocho filtros globales.

Para construir un set de filtros global, se accede a la etiqueta **"Global Sets"**. (Ver figura 2.33). En primer lugar, se hace clic sobre el botón "Refresh" para actualizar los valores por si ha habido cambios en la información de las otras etiquetas que afecten a los sets de filtros globales ya definidos. Seguidamente, se hace clic en el botón "Insert", y se abre la caja de diálogo para construir un nuevo set de filtros global.

Figura 2.33: Etiqueta "Global Sets". Información de los sets globales.

En la figura 2.34 se muestra la caja de diálogo para construir un set de filtros global. En ella se le asigna un Id, un nombre y se hace clic sobre el botón de puntos suspensivos del campo **FilterIdList** para seleccionar los filtros globales que pertenecerán al set global que se está construyendo. Finalmente, se hace clic en el botón **"Insert"** de la caja de diálogo, y listo. Se observa que la numeración de los identificadores está comprendida del 1 al 100, siendo 100 el total de sets de filtros globales.

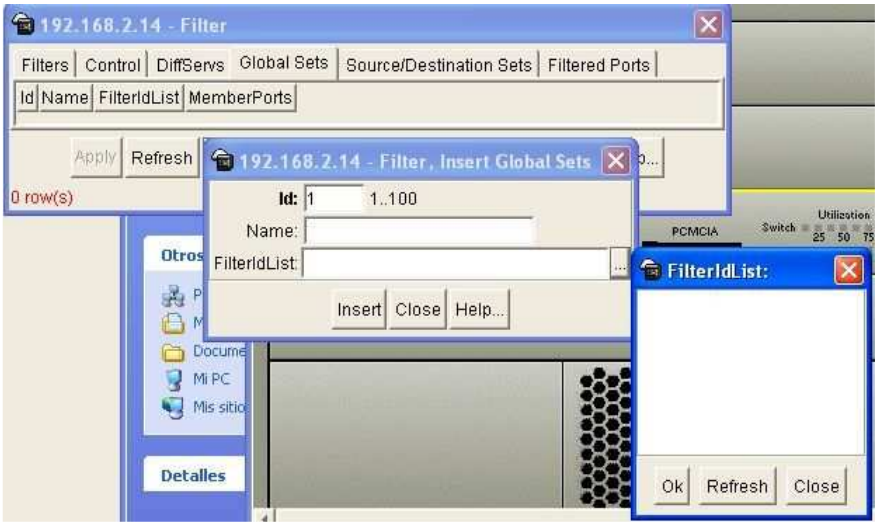


Figura 2.34: Etiqueta "Global Sets". Caja de diálogo de un set de filtros global.

2.3.1.3.2 Construcción de Sets de Filtros Origen/Destino

Para construir un set de filtros origen/destino, se accede a la etiqueta **"Source/Destination Sets"**. (Ver figura 2.35). En primer lugar, se hace clic sobre el botón "Refresh" para actualizar los valores por si ha habido cambios en la información de las otras etiquetas que afecten a los sets de filtros origen/destino ya definidos. Seguidamente, se hace clic en el botón **"Insert"**, y se abre la caja de diálogo para construir un nuevo set de filtros origen/destino.

Figura 2.35: Etiqueta "Source/Destination Sets". Información de los sets origen/destino.

En la figura 2.36 se muestra la caja de diálogo para construir un set de filtros origen/destino. En ella se le asigna un Id, un nombre y se hace clic sobre el botón de puntos suspensivos del campo **FilterIdList** para seleccionar los filtros origen/destino que pertenecerán al set origen/destino que se está construyendo. Finalmente, se hace clic en el botón **"Insert"** de la caja de diálogo, y listo. Se observa que la numeración de los identificadores está comprendida del 300 al 1000, siendo 700 el total de sets de filtros origen/destino.

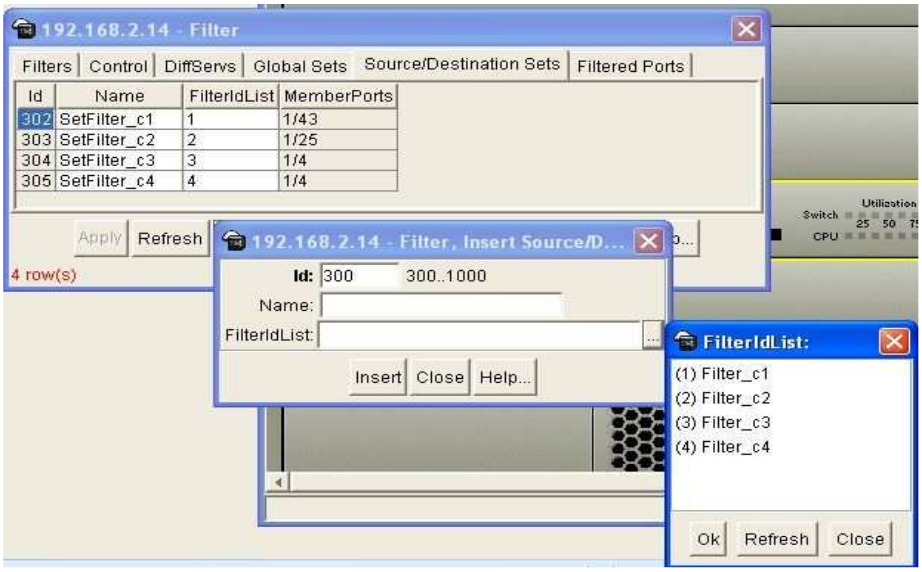


Figura 2.36: Etiqueta **"Source/Destination Sets"**. Caja de diálogo de un set origen/destino.

Por ejemplo, en la figura 2.35 se muestra que el set de filtros nombrado "SetFilter_c2" se le ha asignado el identificador Id 303, se observa que a este set sólo pertenece un filtro que está identificado por el id número 2, y el puerto al que se aplica es el número 25.

2.3.1.3.3 Aplicación a un puerto o un conjunto de puertos

El siguiente paso tras la construcción de sets de filtros, consiste en **aplicar dichos sets de filtros a un puerto o a un conjunto** de puertos. Para ello, se accede a la etiqueta **"Filtered Ports"**. (Ver figura 2.37).
En primer lugar, se hace clic sobre el botón "Refresh" para actualizar los valores por si ha habido cambios en la información de las otras etiquetas que afecten al filtrado de puertos. Seguidamente, se hace clic en el botón **"Insert"**, y se abre la caja de diálogo para asociar puertos con los sets de filtros construidos (Ver figura 2.38). Se hace clic sobre el botón de puntos suspensivos del campo **FilterSet** y aparece la lista de todos los sets de filtros tanto globales como origen/destino construidos. De entre ellos se seleccionan los que se deseen aplicar sobre el puerto o conjunto de puertos deseados. A continuación, se hace clic sobre el botón de puntos suspensivos del campo **Ports** y aparece la lista de los cuarenta y ocho identificadores de los cuarenta y ocho puertos físicos del equipo *Passport 8600 Routing Switch*. Se selecciona/n el puerto o puertos al/los que se quiere aplicar el/los set/s de filtros seleccionado. Se hace clic en OK. Se activa el campo Enable para activar los filtros del/los set/s de filtros seleccionado. En el campo "*DefaultAction*" se selecciona la acción por defecto del/los set/s de filtros seleccionado/s: **forward**, **drop** o **none**. Finalmente, se hace clic en el botón **"Insert"** de la caja de diálogo, y listo.

Nota: Siempre que se cambie un parámetro de un filtro, se debe primero desactivar su set de filtros en la etiqueta **"Filtered Ports"**, y una vez hecho el cambio, a continuación activar su set de filtros de nuevo para volver a aplicar los puertos asociados con el filtro en cuestión.

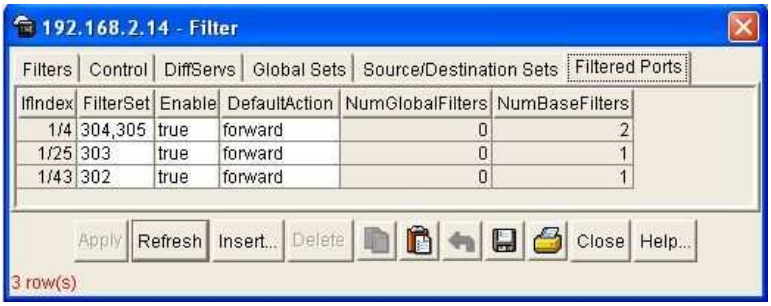


Figura 2.37: Etiqueta "Filtered Ports". Información de los puertos asociados con los filtros definidos.

En la figura 2.38 se muestra la caja de diálogo para aplicar un set de filtros a un puerto o conjunto de puertos.

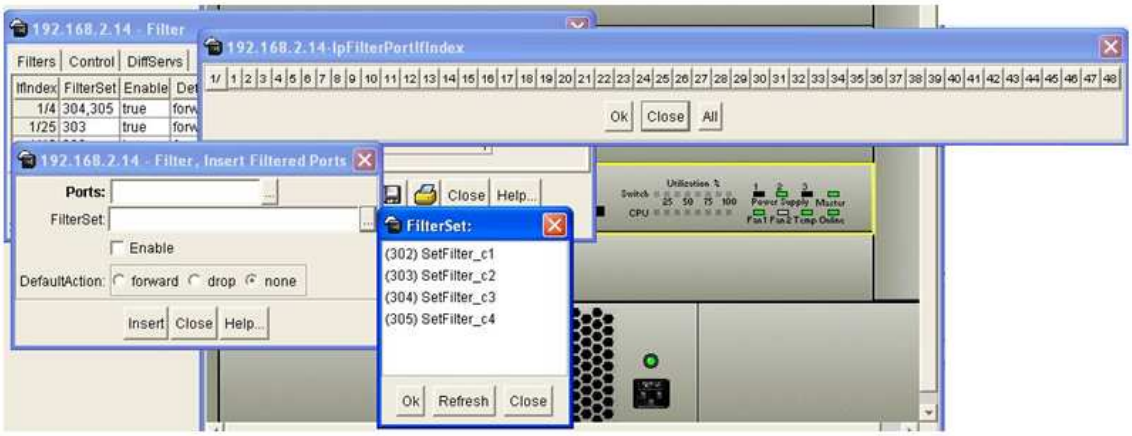


Figura 2.38: Etiqueta **"Filtered Ports"**. Caja de diálogo para asociar puertos a sets de filtros.

Por ejemplo, en la figura 2.37 se muestra que al puerto número 4 se les aplica los sets de filtros cuyos identificadores son 304 y 305. Su acción por defecto es reenviar todos los paquetes que coincidan con los parámetros de coincidencia de los filtros. El campo **NumGlobalFilters** está a 0, ya que no se aplica ningún filtro global al puerto número 4. El campo **NumBaseFilters** está a 2, ya que son dos los filtros origen/destino que se aplican al puerto número 4.

2.3.1.4 Definición y configuración de la función *Traffic Policing* y de Perfiles de Tráfico

La función de policía (*Traffic policing*) es el proceso de asignar una **tasa de tráfico** a un microflujo o a un agregado de flujos cuando atraviesa una red *DiffServ*. El valor de esta tasa se define dentro de un **perfil de tráfico**. La herramienta "perfil de tráfico" del equipo, realiza las funciones de **medidor**, **marcador** y **descartador** (ver figura 2.39). Por tanto, se ocupa de **acondicionar** el tráfico: mide la velocidad o tasa media a la que llegan los paquetes, para así **determinar la conformidad con los parámetros de tráfico** y disparar una **acción** particular. Si la tasa está dentro del valor definido en el perfil, es decir, el paquete es in-profile, los paquetes son marcados con el valor **in-profile DSCP establecido**. Si la tasa excede el valor definido, o bien los paquetes son marcados con el valor **out-of-profile DSCP establecido**, o bien son descartados, en base a la acción definida en el perfil de tráfico. También es posible configurar el perfil de tráfico para que no realice ninguna acción sobre el tráfico.

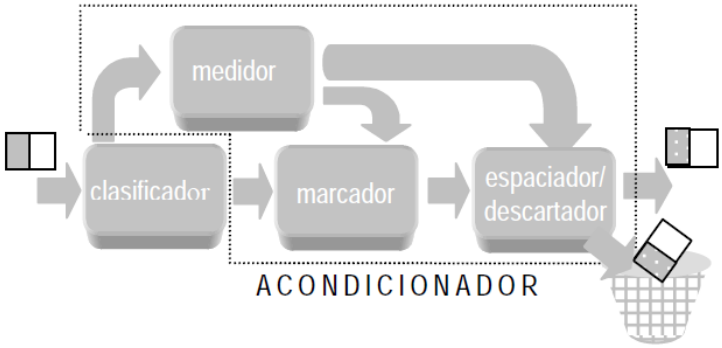
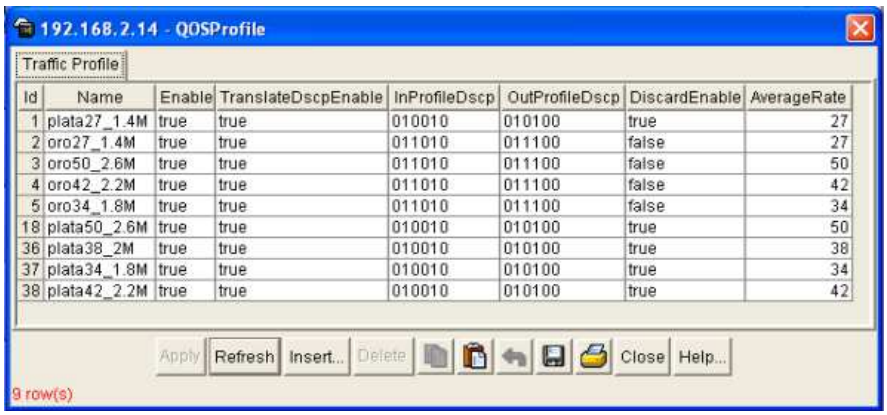


Figura 2.39: Clasificador y elementos lógicos de un acondicionador de tráfico.

La aplicación de un perfil de tráfico sobre un paquete, hace que el paquete sea colocado en una cola de servicio, de acuerdo con su marcado DSCP, lo cual a su vez determina el PHB específico que recibirá. Es decir, un perfil de tráfico especifica el **tratamiento de las propiedades** de un flujo de tráfico seleccionado mediante un **clasificador**. Proporciona **reglas** para determinar si un paquete en particular está dentro o fuera del perfil. Esta determinación se traduce en la **"vigilancia"** de los paquetes IP dentro de un flujo de tráfico, es decir, en la aplicación de una Función de Policía (*Token Bucket*) a cada paquete IP entrante para hacer cumplir el contrato SLA establecido entre el cliente y el proveedor de servicios. El objetivo de acondicionar los flujos de tráfico es hacer cumplir el perfil de tráfico siguiendo una **política de descarte**.

En la política es donde se asocia todo, es decir, cada política engloba un puerto o conjunto de puertos, un set de filtros o conjunto de sets de filtros y un perfil de tráfico que realiza las acciones de medidor, marcador y descartador. Por tanto, la política especifica el tipo de comportamiento, el PHB, que se desea aplicar a un flujo de paquetes.

Para configurar un perfil de tráfico, desde la barra de menú de Device Manager se selecciona **QoS > Profile**, y se abre la caja de diálogo. En ella se visualiza la información de los perfiles de tráfico ya configurados. (Ver figura 2.40).



Id	Name	Enable	TranslateDscpEnable	InProfileDscp	OutProfileDscp	DiscardEnable	AverageRate
1	plata27_1.4M	true	true	010010	010100	true	27
2	oro27_1.4M	true	true	011010	011100	false	27
3	oro50_2.6M	true	true	011010	011100	false	50
4	oro42_2.2M	true	true	011010	011100	false	42
5	oro34_1.8M	true	true	011010	011100	false	34
18	plata50_2.6M	true	true	010010	010100	true	50
36	plata38_2M	true	true	010010	010100	true	38
37	plata34_1.8M	true	true	010010	010100	true	34
38	plata42_2.2M	true	true	010010	010100	true	42

Figura 2.40: Información de los Perfiles de Tráfico definidos.

Para crear un nuevo perfil de tráfico, se hace clic sobre **"Insert"**, y se abre la caja de diálogo, (ver figura 2.41) donde se le asigna un **Id**, un **nombre**, se activa el campo **Enable** para activar el perfil, se activa el campo **TranlateDSCPEnable** para realizar el remarcado de los paquetes que caen dentro y fuera del perfil con el valor DSCP correspondiente definido para ambos casos. A continuación, se introducen dichos valores DSCP de 6 bits en los campos **InProfileDscp** y **OutProfileDscp**. El campo **DiscardEnable** se activa si se desea que los paquetes que no estén dentro del perfil sean descartados.
Por último, se establece la tasa media de tráfico en el campo **AverageRate**, la cual se lleva a cabo en incrementos de 64 bytes cada 2.5 millonésimas de segundo.
Nota: Para introducir el valor de la Tasa Media, se deben realizar unos cálculos basados en unas tablas tabuladas. Estos cálculos se explican en el Capítulo 3.

- **InProfileDscp** → especifica el valor DSCP para los paquetes "buenos", esto es, para los paquetes que cumplen el contrato. Un valor de (000000) significa dejar el campo DSCP sin cambios.

- **OutProfileDscp** → especifica el valor DSCP para los paquetes "violation", esto es, para los paquetes que superen la tasa de lo contratado. Un valor de (000000) significa dejar el campo DSCP sin cambios.

Finalmente, se hace clic en el botón **"Insert"** de la caja de diálogo, y listo.

Nota: Se observa que la numeración de los identificadores está comprendida del 1 al 64, siendo 64 el total de perfiles de tráfico que se pueden definir, y que se pueden aplicar por cada puerto ya que tenemos un total de 64 combinaciones por los 6 bits del código DSCP ($2^6 = 64$).

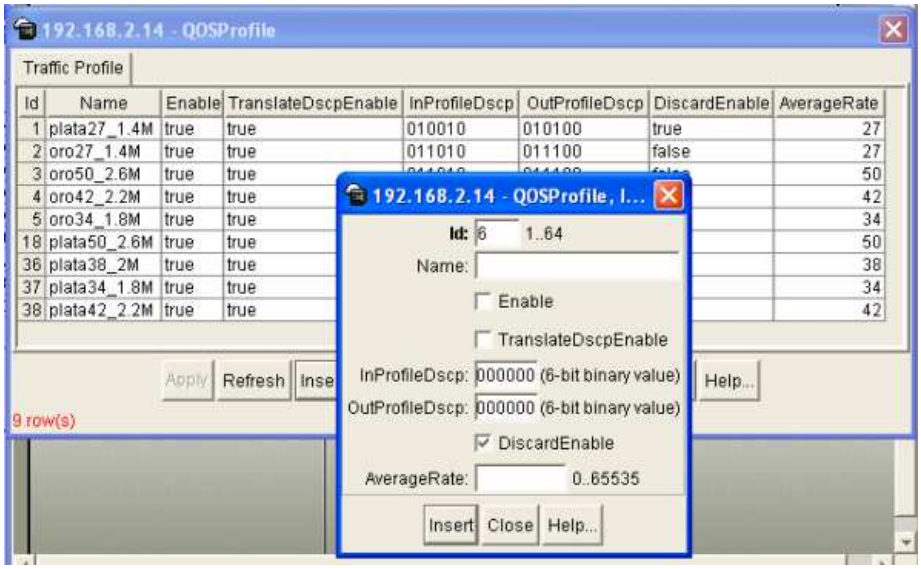


Figura 2.41: Caja de diálogo para definir un Perfil de Tráfico.

Por ejemplo, en la figura 2.40 para el perfil de tráfico nombrado **"plata38_2M"** se le ha asignado el Id número **36**. Está activado, por tanto se aplica el perfil al/los filtro/s a los que haya sido asociado. Realiza el remarcado de los paquetes que caen dentro y fuera del perfil con el valor DSCP correspondiente definido para ambos casos: '010010' para los paquetes que caen dentro del perfil y '010100' para los paquetes que caen fuera del perfil. Los paquetes que no estén dentro del perfil serán descartados. Por último, el valor calculado e introducido en el campo "AverageRate" para que la tasa de tráfico sea aproximadamente de **2 Mbps** es el **38**.

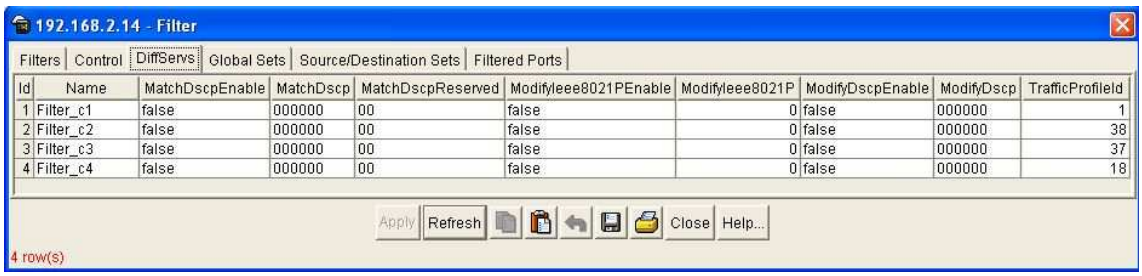


Figura 2.42: Asignación de un Perfil de Tráfico a cada flujo de tráfico filtrado.

En la figura 2.42 se visualiza la asociación a cada flujo de tráfico identificado con un "perfil de tráfico" definido, introduciendo el valor de su identificador en el campo TrafficProfileId.

En resumen, con las herramientas *DiffServ* configuradas en el *Passport 8600 Routing Switch*, se utilizan políticas para dirigir el tráfico mediante la asignación de los paquetes a determinadas colas. El sistema marca el campo *DiffServ* (DS) de los paquetes IP para definir el tratamiento de los paquetes en su viaje a través de la red. Cada flujo de tráfico tras su clasificación y acondicionado mediante la aplicación de políticas recibe un nivel prioridad frente al resto de flujos de tráfico. Se pueden especificar un número de políticas, y en cada política pueden coincidir uno o muchos flujos soportando complejos escenarios de clasificación.

Es por tanto, **la política** el factor global de QoS que interactúa con un grupo de paquetes. Se configuran políticas que monitorizan las características del tráfico y ejecutan una **acción de control sobre el tráfico** cuando ciertas características definidas por el usuario coinciden. El fin de una política es controlar el ancho de banda del enlace, en situación de congestión, mediante la limitación de la cantidad de tráfico que llega de un usuario específico. Este control lo realiza empleando el descarte de los paquetes que están fuera del perfil de tráfico que se aplica, o bien, bajando o subiendo la prioridad (el nivel de QoS) de los paquetes.

Capítulo 3

Pruebas Experimentales

3.1 Introducción

Este capítulo se centra en la toma de una serie de **medidas de tráfico** para evaluar la QoS en la red de datos desplegada en el laboratorio. En primer lugar, se describe la topología de red sobre la que se realizarán las diferentes pruebas. Seguidamente, para cada prueba se describe y expone la configuración del escenario, donde se incluye a qué tasa se genera tráfico y el tipo de tráfico generado (fuentes TCP/UDP). También se explica qué **mecanismos de cola** aplica el router sobre el tráfico. Por último, se muestra el análisis de los resultados obtenidos en cada una de las pruebas experimentales realizadas.

Esta fase del proyecto consiste en recopilar datos durante un periodo de tiempo, empleando y sin emplear las herramientas que Nortel proporciona para implementar la diferenciación de servicios *"DiffServ"* y así medir el **grado de éxito** de la solución implementada. El objetivo es conseguir garantizar el ancho de banda que los usuarios han contratado, y así, que estén satisfechos con el servicio que están recibiendo, según [19].

El experimento consiste en una **competición** de los diferentes tipos de datos generados por el **ancho de banda en el enlace final**, donde tiene lugar una situación de **congestión**, esto es, se degradan las prestaciones de la red. Se espera comprobar que el tráfico de alta prioridad no es retardado por el de baja prioridad y que los clientes con mayor contrato tengan mayor prioridad de descarte, es decir, que sufran menos descartes que aquellos clientes cuyo contrato es menor.

3.2 Despliegue y configuración de la Topología de la red de datos

La **topología de la red** de datos estudiada, consiste en cuatro clientes que generan tráfico hacia un servidor destino, pasando a través de unos nodos que filtran, procesan y encaminan dicho tráfico. Estos nodos son los equipos Nortel: el switch BPS 2000 (*Bussiness Policy Switch 2000*) y el router *Passport 8600 Routing Switch*.
La conexión entre los equipos (*hosts*, switch y router), es la siguiente: dos de los clientes C1 y C2 y el servidor se conectan directamente al router, los otros dos clientes C3 y C4 se conectan al switch, y por último, el switch está conectado al router. Por tanto, el tráfico generado por los clientes C1 y C2 sólo atraviesa el router para llegar al servidor, mientras que el tráfico generado por los clientes C3 y C4 además de por el router pasa por el switch para llegar al servidor, como se muestra en la figura 3.1.

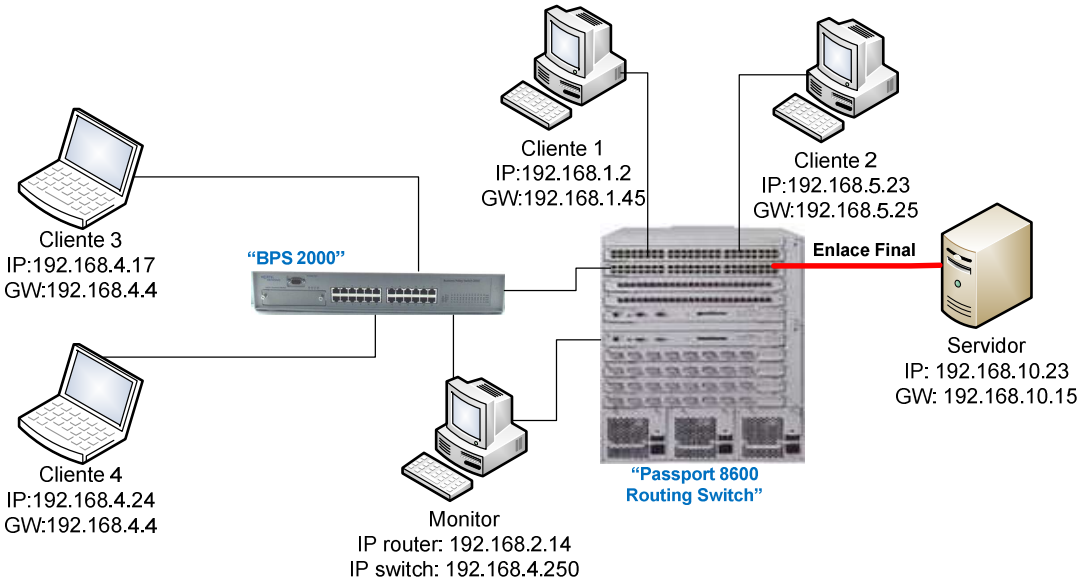


Figura 3.1: Topología física de la red de datos desplegada en el laboratorio.

Tras la descripción de la conexión física de los equipos se procede a la **configuración de la red**. Para configurar la red, partimos de la configuración de los PCs o *hosts* que la constituyen. Seguidamente, se configurarán las direcciones IP de los nodos Nortel y las direcciones IP de las interfaces (puertos) del router a las que están conectados los clientes y el servidor.
Simplemente se tienen que configurar las direcciones IP de las tarjetas de red de cada uno de los *hosts* y sus gateways correspondientes. Por un lado, están las tarjetas de red que hacen de ***fuentes generadoras del tráfico*** que es objeto de nuestro estudio y la tarjeta de red del servidor. Por otro lado, están las tarjetas de red del PC que monitoriza los equipos de conmutación: el switch BPS 2000 y el router *Passport 8600 Routing Switch*.
Los PCs que hacen de fuentes generadoras (clientes) y el PC que hace de servidor, tienen como sistema operativo la versión 8.0 de la distribución de *Linux* Suse. Para configurar sus tarjetas de red se utilizará la **herramienta Yast2**. El procedimiento es el siguiente:

1. Lanzar la herramienta

2. Seleccionar "Configuración de la tarjeta de red" del menú Red/Básica (Ver figura 3.2)

Figura 3.2: Herramienta Yast2. Configuración de tarjetas de red.

3. Asignar las direcciones IP a cada tarjeta generadora de tráfico y las direcciones IP de sus *gateways* correspondientes, para cada cliente (Ver tabla 3.1).

Tabla 3.1: Direcciones IP y *gateways* asignadas.

HOST	@IP	MÁSCARA	INTERFAZ	GATEWAY
Cliente 1	192.168.1.2	255.255.255.0	eth0	192.168.1.45
Cliente 2	192.168.5.23	255.255.255.0	eth0	192.168.5.25
Cliente 3	192.168.4.17	255.255.255.0	eth0	192.168.4.4
Cliente 4	192.168.4.24	255.255.255.0	eth0	192.168.4.4
Servidor	192.168.10.23	255.255.255.0	eth0	192.168.10.15

Nota: La puerta de enlace (gateway) de cada tarjeta de red debe ser la @IP asignada al puerto del router al que se conecta.

El PC que monitoriza el router y el switch, tiene dos tarjetas de red. Su sistema operativo es Windows XP. En la figura 3.3 se visualiza las direcciones IP asignadas y sus gateways correspondientes:

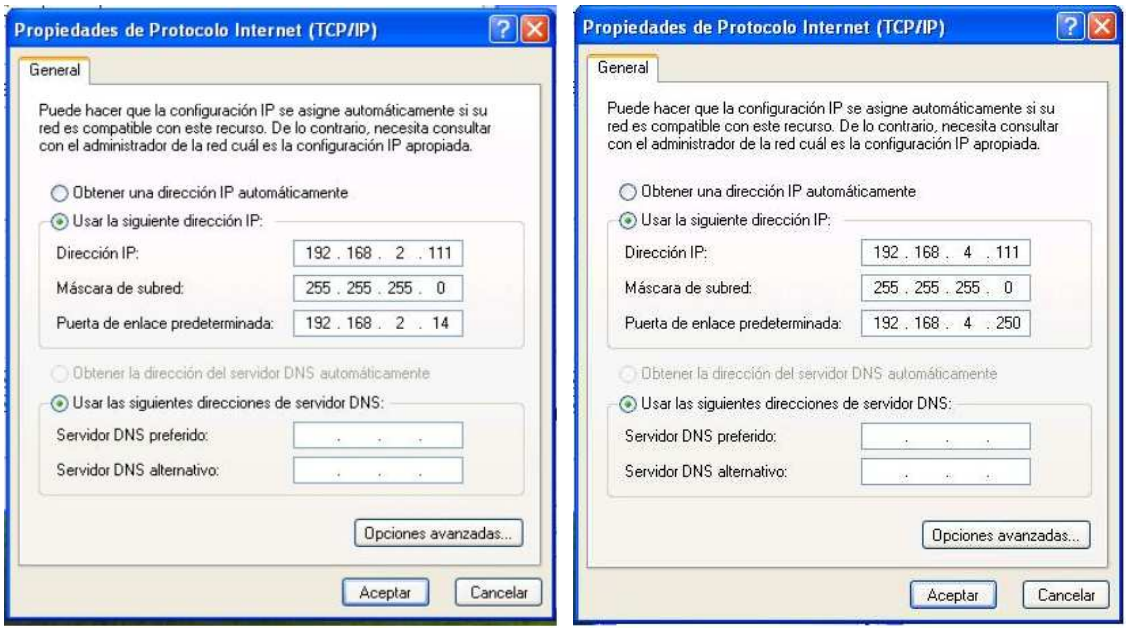


Figura 3.3: Configuración de tarjetas de red del equipo de monitorización.

Nota: las direcciones IP de las *gateways* se corresponden con las direcciones IP de los equipos *Passport 8600 Routing Switch* y BPS 2000 (Tabla 3.2):

Tabla 3.2: Direcciones IP de los equipos Nortel.

EQUIPO	@IP
Passport 8600 Routing Switch	192.168.2.14
BPS 2000	192.168.4.250

Nota[1]: Para ver cómo se configuran las direcciones IP de los equipos Nortel ir al capítulo 2 al apartado **"2.2.3 Puesta en Marcha del Equipo"**.

Nota[2]: La configuración de los puertos del router se explica en el capítulo 2 en el apartado **"2.3.1.1 Activación del campo *"DiffServEnable"*, selección del tipo de puerto *"core/access"* y asignación de dirección IP"**.

En la tabla 3.3 se muestran las direcciones IP asignadas a los puertos del router a los que se conectan los clientes y el servidor:

Tabla 3.3: Direcciones IP de los puertos del router.

PUERTO	@IP	MÁSCARA	HOST
45	192.168.1.45	255.255.255.255	Cliente 1
25	192.168.5.25	255.255.255.255	Cliente 2
4	192.168.4.4	255.255.255.255	Cliente 3
4	192.168.4.4	255.255.255.255	Cliente 4
15	192.168.10.15	255.255.255.255	Servidor

Nota: La @IP asignada a cada puerto se corresponde con la puerta de enlace (gateway) de la correspondiente tarjeta de red del host al que se conecta.

3.3 Pruebas Experimentales: Escenarios, Servicio de Colas y Resultados

3.3.1 Escenarios

Se van a diferenciar **dos tipos** de **escenarios** generales:

1. Configuración con una cola (plata)
2. Configuración con dos colas (plata y oro).

Para la configuración con una cola (plata) se sigue el siguiente **esquema de pruebas experimentales:**

A. Sin aplicar Servicios Diferenciados (sin activar DROP)

   a. Mismo contrato
      i. Tráfico generado TCP
      ii. Tráfico generado UDP y TCP

   b. Distintos contratos
      i. Tráfico generado TCP
      ii. Tráfico generado UDP y TCP

B. Aplicando Servicios Diferenciados (se activa DROP)

   a. Mismo contrato
      i. Tráfico generado TCP
      ii. Tráfico generado UDP y TCP

   b. Distintos contratos
      i. Tráfico generado TCP
      ii. Tráfico generado UDP y TCP

Para la configuración con dos colas (plata y oro) se sigue el siguiente **esquema de pruebas experimentales:**

- Sin aplicar Servicios Diferenciados (sin activar DROP)

    a. Distintos contratos
        i. Tráfico generado UDP y TCP:
            - contratos fuentes TCP C2 y C4 > contratos fuentes UDP C1 y C3

        ii. Tráfico generado UDP y TCP
            - contratos fuentes TCP C2 y C4 < contratos fuentes UDP C1 y C3

- Aplicando Servicios Diferenciados (se activa DROP)

    a. Distintos contratos
        i. Tráfico generado UDP y TCP:
            - contratos fuentes TCP C2 y C4 > contratos fuentes UDP C1 y C3

        ii. Tráfico generado UDP y TCP:
            - contratos fuentes TCP C2 y C4< contratos fuentes UDP C1 y C3

La configuración de cada escenario, tiene lugar en el router a través del software de red *Device Manager* instalado en un PC que monitoriza el tráfico que entra y sale del router. Los pasos a seguir para establecer las distintas configuraciones son los siguientes:

1) En primer lugar, hay que definir **los filtros** para diferenciar el tráfico total que llega al router en los flujos de tráfico correspondientes a cada cliente.

2) En segundo lugar, se configuran **los contratos** de los clientes, es decir, el ancho de banda máximo acordado con el proveedor de servicios que cada uno de los clientes contrata del enlace final. Para ello, según [14], el router *Passport 8600 Routing Switch*, dispone de tres tablas tabuladas (10 Mbps Ethernet, 100 Mbps Fast Ethernet y 1 Gigabit Ethernet), según **la velocidad del enlace** y según el **tamaño del paquete** en bytes, que ilustran el *throughput* efectivo (tasa de envío de datos sin *overhead*) en Mbps para **varios flujos de tráfico usando diferentes valores umbrales de la tasa contratada** (Ver tablas 3.4, 3.5 y 3.6).

    En el *Passport 8600 Routing Switch*, la medida de la velocidad (tasa) de QoS se lleva a cabo en incrementos de 64 bytes cada 2,5 milésimas de segundos. Las tablas presentan las **velocidades de los enlaces medidas**, en **múltiplos de 64**, para las tres velocidades *Ethernet* probadas, con los resultados esperados. Sobre estos resultados se deben tener en cuenta dos consideraciones respecto al ancho de banda:

    a. El conmutador reenvía los paquetes enteros, incluso si sólo se ha recibido parte del paquete (paquetes de longitud fija, **padding**).

    b. El *Ethernet overhead*, IPG (*InterPacket Gap*) y el preámbulo, debe ser sustraído de la velocidad total.

Tabla 3.4: "*Throughput* efectivo en enlace de 10 Mbps Ethernet"

Tamaño del paquete en bytes	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
64	1.03	2.05	3.08	4.10	5.12	6.15	7.17	7.62	7.62	7.62
128	1.23	2.05	3.28	4.10	5.33	6.15	7.38	8.20	8.65	8.65
256	1.64	2.46	3.28	4.10	5.74	6.56	7.38	8.19	9.28	9.28
512	1.64	3.28	3.28	4.92	6.56	6.56	8.20	8.20	9.62	9.62
1024	3.28	3.28	3.28	6.56	6.56	6.56	9.81	9.81	9.81	9.81
1518	4.86	4.86	4.86	4.86	9.72	9.72	9.72	9.72	9.72	9.87

Tabla 3.5: "*Throughput* efectivo en enlace de 100 Mbps Fast Ethernet"

Tamaño del paquete en bytes	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
64	10.25	20.49	30.74	40.99	51.23	61.15	71.72	76.19	76.19	76.19
128	10.25	20.49	30.74	40.99	51.24	61.48	71.72	81.97	86.49	86.49
256	10.66	20.47	31.11	40.93	51.58	61.40	72.04	81.97	92.62	92.75
512	11.48	21.32	31.15	40.99	52.46	62.29	72.13	81.97	93.44	96.24
1024	13.12	22.96	32.80	42.63	52.46	62.30	72.13	81.97	95.08	98.08
1518	14.58	24.31	34.02	43.75	53.47	68.05	77.77	87.49	97.20	98.70

Tabla 3.6: "*Throughput* efectivo en enlace de Gigabit Ethernet"

Tamaño del paquete en bytes	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
64	102.50	205.00	307.47	409.93	446.61	446.61	446.61	446.61	446.61	446.61
128	102.50	204.93	307.43	409.95	512.38	614.80	717.24	819.67	922.11	927.54
256	102.49	204.96	307.43	409.95	512.38	614.80	717.24	819.67	922.11	927.54
512	103.32	204.99	308.30	409.86	513.13	614.79	718.07	819.68	922.93	962.41
1024	104.92	206.57	308.23	409.96	514.85	616.45	718.07	819.68	924.57	980.84
1518	106.93	213.89	320.90	422.93	529.87	636.78	743.68	845.72	952.62	986.99

Según lo explicado, suponiendo una velocidad del enlace de 10 Mbps y un tamaño de paquete P=1518 bytes, si se quiere obtener el throughput al 100%, se selecciona de la tabla 3.4 "*Throughput* efectivo en enlace de 10 Mbps Ethernet" el **valor 9,87** que se corresponde con un tamaño de paquete P=1518 bytes y con un throughput del 100% del enlace. Al hacer los cálculos se obtiene:

1518 bytes * **9,87** * 64 bytes * 8 bits/byte = 7,67 Mbps **(1)**

Este valor del throughput es inferior a los 10 Mbps que se deberían obtener. Esta disminución del ancho de banda se debe a que el *overhead* (IPG y preámbulo) generado por el paquete es sustraído.

Por lo tanto, para calcular el **valor** correspondiente al máximo ancho de banda que se quiere contratar para un cliente dado, se despeja de la ecuación **(1)** y se procede con la siguiente fórmula:

$$\textbf{valor} = \textbf{BW} / (\textbf{P} * \textbf{64 bytes} * \textbf{8 bits}) \quad \textbf{(2)}$$

Siendo:

BW: ancho de banda que se desea contratar
P: tamaño del paquete bytes

Por ejemplo, para saber el valor que se corresponde con un contrato de **2 Mbps** para un enlace de 10 Mbps y un tamaño de paquete P = 1024 bytes, sería:

$$\textbf{valor} = 2000000/(1024*64*8) = \textbf{3,814} \quad \textbf{(3)}$$

Ahora, buscamos en la **tabla de 10 Mbps Ethernet** el valor obtenido en **(3)**. El 20% de 10 Mbps es 2 Mbps que es el ancho de banda que queremos conseguir, por lo que para determinar el valor se escoge la columna del 20% y la fila para un tamaño de paquete de 1024 bytes. Se observa que el valor determinado en la tabla **3,28**, se aproxima al obtenido en **(3)**, con lo cual los cálculos realizados son correctos. Este valor **aparece repetido** en las columnas del 10%, del 20% y del 30% del ancho de banda total del enlace. Este hecho limita la **precisión** de seleccionar el ancho de banda límite contratado que se desee asignar a un cliente dado, ya que con un valor de 3,28 se obtiene un caudal de:

1024 bytes * 3,28 * 64 * 8 = **1,72** Mbps

Además, el valor que se debe introducir para la configuración de los contratos en el router debe ser un **número entero**, por lo que se redondea el valor calculado en la fórmula **(2)**. Así para un valor de 3 se obtiene:

1024 bytes * **3** * 64 * 8 = **1,57 Mbps**

Y con un valor de 4 se obtiene:

1024 bytes * **4** * 64 * 8 = **2,097 Mbps**

Que es el throughput deseado.

En un escenario en el que se quiera jugar con distintos valores para **asignar diferentes contratos** a cada cliente, la tabla 3.4 "*Throughput* efectivo en enlace de 10 Mbps Ethernet", limita el rango de poder escoger entre diferentes valores, ya que como hemos visto los valores se repiten en varias columnas de diferentes porcentajes del ancho de banda del enlace.

Así para el caso "Diferentes Contratos", se ha configurado que **los puertos** de todos los clientes vayan a **100 Mbps** y que el puerto del servidor destino vaya a 10 Mbps (ancho de banda del enlace destino). De este modo, se puede **jugar con un mayor margen de valores**. (Ver tabla 3.5 "*Throughput* efectivo en enlace de 100 Mbps Fast Ethernet"). En esta tabla no se repiten los valores para diferentes porcentajes del ancho de banda del enlace.

De esta forma, para calcular los valores que se van a introducir para configurar los contratos en el escenario **"Diferentes Contratos"** tendremos (Ver tabla 3.7):

Tabla 3.7: Valores calculados para configurar el escenario "Distintos Contratos"

BW CONTRATADO	CÁLCULO DEL VALOR EN ENLACE DE 10 MEGAS	VALOR EN ENLACE 100 MEGAS
1,4 Mbps	**valor** =1400000/(1024*64*8) = 2,67	26,7 ≈ **27**
1,8 Mbps	**valor** = 1800000/(1024*64*8) = 3,43	34,3 ≈ **34**
2,2 Mbps	**valor** = 2200000/(1024*64*8) = 4,19	41,9 ≈ **42**
2,6 Mbps	**valor** = 2600000/(1024*64*8) = 4,95	49,5 ≈ **50**

Asimismo, para el escenario **"Mismo Contrato"** se ha calculado el valor situándonos en el mismo contexto (enlaces de los clientes a 100 Mbps y enlace final a 10 Mbps):

2 Mbps → **valor** = 2000000/(1024*64*8) = 3,81 → enlace 100 Mbps 38,1 ≈ **38**

Comprobación:

1024*64*8*__38__ = 19922944 = 20M para enlace a 100M → 2M para enlace a 10M

Los clientes van a generar tráfico a 1,25 Mbps, 2 Mbps y 3 Mbps, por ello el enlace final se ha configurado a 10 Mbps. Los enlaces de los clientes van a 100Mbps únicamente para poder optar a un mayor rango de valores para configurar sus contratos, y el poner el enlace final a 10 Mbps hace que los valores calculados sean equivalentes a contratos correspondientes a la tabla de 10 Mbps.

3.3.2 Servicio de Colas: Encolamiento y Prioridades de Servicio.

Según [15], en una red *DiffServ* el tráfico es clasificado conforme entra a la red y se le asigna un PHB (comportamiento por salto) basado en dicha clasificación. El PHB impone el **drop precedence** (la prioridad de descarte) y la **latencia** (la prioridad de emisión) que experimenta un **flujo de datos**.

Según [17] y [20], existen dos conceptos que definen la base para la **gestión del tráfico**: la prioridad de emisión y la prioridad de descarte. Estos conceptos están indirectamente relacionados. La prioridad de emisión define la **urgencia del tráfico**. Mientras que la prioridad de descarte define la **importancia del tráfico**. Un paquete con alta prioridad de emisión implica que este paquete sea servido primero. Un paquete con alta prioridad de descarte implica que este paquete debe ser el último en ser descartado en caso de congestión. Por ejemplo, el tráfico sensible al retardo como la voz y el vídeo debería ser clasificado con alta prioridad de emisión, mientras que el tráfico sensible a la pérdida de paquetes como la información financiera debería ser clasificado con alta prioridad de descarte. En el Passport 8600 la prioridad de emisión y la prioridad de descarte son comúnmente referidas como la latencia y el drop precedence, respectivamente.

Dependiendo del nivel de prioridad de cada paquete, el conmutador los va introduciendo en la cola apropiada. Para transmitir los paquetes de cada cola, el Passport 8600 implementa los **"mecanismos de encolamiento": *Strict Priority Queuing*** para la Clase de Servicio *Premium* y **WRR** (Weighted Round Robin) para el resto de niveles, colas o clases de servicio.

3.3.2.1 Mecanismos de encolamiento: Strict PQ y WRR

El conmutador Passport 8600 proporciona al tráfico que llega a cada puerto ocho **niveles** de QoS, u ocho **colas hardware**, u ocho niveles de prioridad de emisión (Ver figura 3.4).
La prioridad de emisión aumenta conforme se sube de nivel o número de cola y se asigna desde el nivel más alto (7) hasta el nivel más bajo (0). Por ejemplo, el tráfico asignado al nivel 5 de QoS tiene mayor prioridad que el tráfico asignado al nivel 4 de QoS.

Así, la cola 0 tiene la más baja prioridad de emisión mientras que la cola 7 tiene la más alta prioridad para ser servida. Estas colas se mapean directamente a los niveles de QoS de 0 a 7 respectivamente. Las colas 6 y 7 se conocen como **colas de "prioridad estricta"**, lo cual significa, que el servicio está garantizado. Las colas de la 1 a la 5 se conocen como **colas Weighted Round Robin** (WRR), lo cual significa, que cada cola se servirá de acuerdo a su **"peso administrativo"** de cola después de que el tráfico de prioridad estricta haya sido completamente servido.

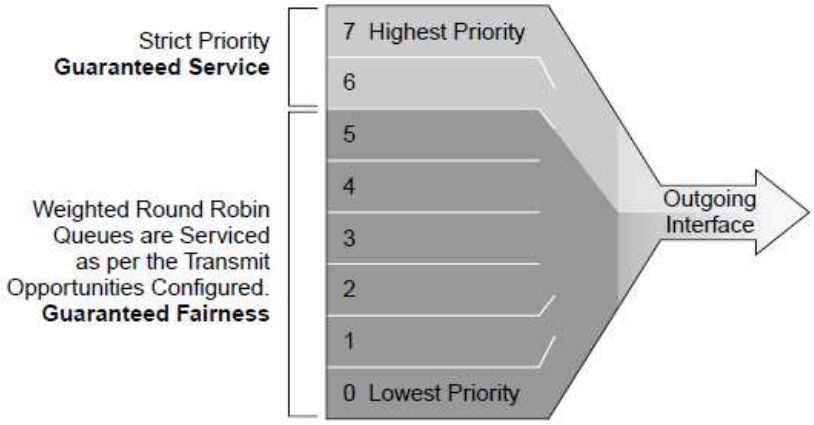


Figura 3.4: Estructura de las colas del *Passport 8600*.

A continuación, se describen los "mecanismos de encolamiento" que implementa el Passport 8600:

- **SPQ *"Strict Priority Queuing"*** (prioridad estricta) asegura que el tráfico de gran prioridad será enviado completamente siempre antes que el de baja prioridad. Se da servicio a las **colas de mayor prioridad en su totalidad**, y sólo entonces se procesan sucesivamente las de prioridad inferior. Dentro de cada una de las colas de prioridad estricta los paquetes se sirven en el orden FIFO (*First-in, first-out*).
  La desventaja está en que el **tráfico de baja prioridad** podría verse **completamente bloqueado**, es decir, puede experimentar un retardo excesivo. Además, si el volumen de tráfico de alta prioridad llega a ser excesivo, se puede descartar el tráfico de baja prioridad cuando las memorias reservadas para este tipo de tráfico se desborden.
  La prioridad estricta garantiza que las aplicaciones para las que el tiempo es muy importante **se reenvíen siempre antes** que las aplicaciones para las que el tiempo no es tan importante. Por ejemplo, un cliente puede querer usar el servicio de voz sobre IP y no quiere que el proveedor de servicios le tire ningún paquete para mantener cierta calidad de servicio en la comunicación. Por tanto, hasta que todo el tráfico de voz sobre IP sea transmitido, no se transmite el tráfico de menor prioridad como puede ser tráfico de correo electrónico (SMTP) o FTP.

- **WRR *"Weighted Round Robin"*** (turno rotativo ponderado): las colas se sirven siguiendo un tiempo en orden *round-robin*, es decir, en orden de prioridad secuencial circular (del primero al último y vuelta al primero). Las colas vacías se saltan. Por tanto, en esta configuración el **tráfico de baja prioridad** no es bloqueado por el de alta prioridad. Garantiza que una sola aplicación no domine la capacidad de reenvío del router. Todas las colas pueden intervenir en el WRR. Soporta flujos con diferentes requerimientos de ancho de banda. Esto lo logra dándole a cada cola un peso que le asigna un porcentaje diferente del ancho de banda de salida.

3.3.2.1.1 Pesos administrativos para las colas de tráfico.

Como se ha descrito en el apartado anterior, el Passport 8600 proporciona al tráfico que llega a cada puerto ocho **niveles** de QoS, u ocho **colas hardware**, u ocho niveles de prioridad de emisión. Cada una de estas colas se corresponde con una **Clase de Servicio**. El sistema calcula un **"peso administrativo"** para cada Clase de Servicio, especificando de este modo el **porcentaje** del ancho de banda del puerto de salida reservado para cada cola. Los pesos administrativos actualmente no son configurables y están asignados a cada cola mediante los **PTOs** (Oportunidades de Transmisión de un Paquete). El Passport 8600 se basa en el **porcentaje de pesos** para configurar la oportunidad de transmitir un paquete por cada cola.

Los **PTOs** indican la probabilidad de que un paquete sea transmitido. Cada PTO es asignado a un slot de tiempo. A cada una de las ocho colas, se pueden asignar hasta **32 slots de tiempo** o PTOs.
Los pesos administrativos se asignan como un **porcentaje** del número total posible de oportunidades de transmitir un paquete. Por ejemplo, un peso administrativo del 100% indica que esta cola tiene 32 oportunidades de transmitir un paquete. Un peso administrativo de 50% indica que esta cola tiene 16 oportunidades de transmitir un paquete, es decir, el 50% de las 32 de oportunidades de transmitir un paquete posibles. La tabla 3.8 proporciona una ilustración de la estructura PTO del Passport 8600.

Tabla 3.8: Estructura PTO del *Passport 8600*.

			Time Slots																															
QoS Lev	**Pto**	**% Wt**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
7	2	6	x	x	Fixed (not configurable)																													
6	32	100	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
5	10	31			x	x	x				x	x	x						x	x	x						x							
4	8	25						x	x					x	x							x	x					x	x					
3	6	18								x						x	x							x	x					x				
2	4	12																x								x					x	x		
1	2	6																															x	x
0	0	0																																

Hay un total de 32 PTOs. La **Cola 7** tiene **2 oportunidades** de las 32 PTOs, dándole aproximadamente un peso del **6%**. La **Cola 6** tiene **32 oportunidades** de las 32 PTOs, dando prácticamente un peso del **100%**. La **Cola 5** tiene **10 oportunidades** de las 32 PTOs, dándole un peso del **31%**. La **Cola 4** tiene **8 oportunidades** de las 32 PTOs, dándole un peso del **25%**. La **Cola 3** tiene **6 oportunidades** de las 32 PTOs, dándole aproximadamente un peso del **18%**. La **Cola 2** tiene **4 oportunidades** de las 32 PTOs, dándole un peso del **12%**. La **Cola 1** tiene **2 oportunidades** de las 32 PTOs, dándole aproximadamente un peso del **6%**. La **Cola 0** tiene **0 oportunidades** de las 32 PTOs, dándole un peso del **0%.**

La principal razón del mecanismo de pesos en las colas y el modo de operación WRR es evitar que las colas de menor prioridad sufran inanición en el servicio respecto a las de alta prioridad, y por tanto no sean servidas.

Los pesos administrativos **controlan** el retardo relativo del tráfico que pasa a través de cada una de las ocho colas de QoS. Cuando llega la oportunidad de transmitir un paquete, esto es, su slot de tiempo y la cola contiene datos, el paquete es servido. Si dos colas contienen datos y sus slots de tiempo llegan al mismo tiempo, la cola con más alta prioridad es servida primero.

Un valor de 32 PTOs implica una probabilidad de transmitir un paquete del 100%. Mayor número de PTOs, o pesos administrativos más altos, se asignan a las colas con alta prioridad, de manera que las transmisiones sensibles al tiempo se transmiten con una **latencia mínima**. Las transmisiones menos sensibles al tiempo o el tráfico de menos prioridad, va a las colas con baja prioridad, a las cuales se les asignan menor número de PTOs, o pesos administrativos más bajos.

En la tabla 3.9 se observa que el peso de cada cola está determinado por lo que se conoce como su PTO. La tabla proporciona un resumen de las configuraciones de cola por defecto junto con sus PTOs y pesos administrativos. Cada fila representa cada uno de los ocho niveles de QoS. Éstos se enumeran del nivel 0 al nivel 7. El nombre de las clases de servicio de tráfico especifica el tratamiento prioritario del tráfico en esta cola. Estos nombres siguen una nomenclatura simple tales como Network, Premium, Platino, Oro, Plata, Bronce, y Standard. En la última columna se expresan los PTOs como un porcentaje del número total (32) de oportunidades de transmitir un paquete.

Tabla 3.9: Mapeo entre Clase de Servicio, nivel de QoS, PHB, PTO y el Porcentaje del Peso

Traffic Service Class	QoS Level	PHB	Packet Transmit Opportunity	Percentage Weight
Network	7		2	6%
Premium	6	Expedited Forwarding	32	100%
Platinum	5	Assured Forwarding	10	31%
Gold	4	Assured Forwarding	8	25%
Silver	3	Assured Forwarding	6	18%
Bronze	2	Assured Forwarding	4	12%
Standard	1	Default	2	6%
User-defined	0		0	0%

Nota: La clase de servicio Network correspondiente a la Cola 7 se reserva para el control de tráfico de red y no es configurable.

La **clase Premium** correspondiente al nivel 6 de QoS se asigna el PHB *Expedited Forwarding*, porque esta clase es para tráfico con requerimientos estrictos de QoS, tales como el tráfico de voz y de vídeo que debe ser transmitido **sin retardos**. Por tanto, la **Cola 6** tiene la más alta oportunidad de transmitir, **32 PTOs** y sus paquetes deben ser completamente servidos y encaminados antes de pasar a servir otra cola. Las **clases Platino, Oro, Plata y Bronce** componen los cuatro grupos del PHB *Assured Forwarding*. La Clase de Servicio **Standard** se corresponde con el PHB por defecto, es decir, que todo el tráfico correspondiente al **nivel 1** de QoS, obtiene el servicio tradicional Best Effort. Por ejemplo, el tráfico de navegación Web se puede colocar en la Cola 1 debido a su baja prioridad y su tolerancia al retardo.
Conforme los paquetes son colocados en las colas, éstas son servidas de acuerdo al mecanismo garantizado *Weighted Round Robin* (WRR). Este mecanismo asegura **prioridad estricta** (*Strict priority*) a la cola asignada a la clase Premium, y el resto de colas son servidas de acuerdo al Turno Rotativo Ponderado WRR (ver tabla 3.10). Este mecanismo se basa en la oportunidad de transmisión de un paquete (PTO, *Packet Transmit Opportunity*) para determinar qué cola se sirve primero.

Tabla 3.10: Mapeo de los Mecanismos de Encolamiento: *Strict Priority* y WRR

Class of Service	Emission queue	Type	Packet transmission opportunity	Percentage weight
Network	7	Strict priority	2	6%
Premium	6	Strict priority	32	100%
Platinum	5	WRR	10	31%
Gold	4	WRR	8	25%
Silver	3	WRR	6	18%
Bronze	2	WRR	4	12%
Standard	1	WRR	2	6%
Custom	0	WRR	0	0%

Básicamente, el programador de cola (*scheduler*) sirve primero bajo el mecanismo ***Strict priority*** la cola 7 hasta el final, entonces pasa al siguiente nivel y sirve la cola 6 hasta su terminación, después

pasa al siguiente nivel para servir las colas WRR en un escenario Round Robin en función de sus pesos. Si una de las colas de "prioridad estricta" recibe un paquete mientras el planificador está sirviendo una de las colas WRR, éste completará el servicio del paquete actual y saltará inmediatamente para servir la cola de prioridad estricta. Una vez que se han servido todos el/los paquete/s en la cola de **prioridad estricta**, el planificador volverá donde lo dejó en el servicio de colas WRR. (Ver figura 3.5)

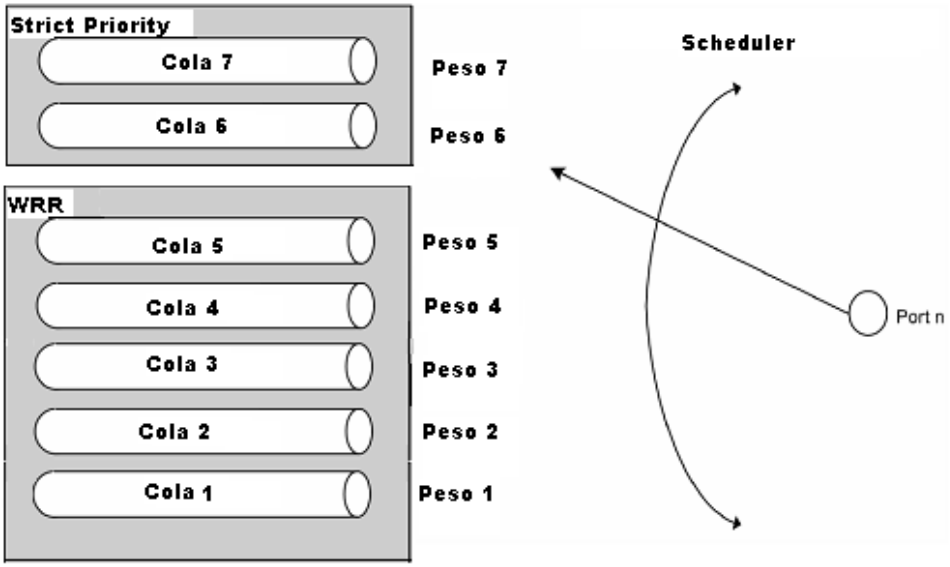


Figura 3.5: Mecanismos de Encolamiento del *Passport 8600*.

Cada cola de salida tiene su propio **peso** que garantiza un **porcentaje** del tiempo de transmisión. Dicho porcentaje se traduce a un valor de ancho de banda. Por ejemplo, el tráfico de voz debería obtener siempre el 100% del ancho de banda, el tráfico vídeo/audio debería obtener entre el 25% y el 31% del ancho de banda, y el tráfico de email debería obtener entre el 13% y el 19% del ancho de banda.

3.3.3 Resultados

A continuación, se muestran los resultados obtenidos en las distintas simulaciones correspondientes a los escenarios configurados. Estos resultados se muestran en forma de **gráficas** que representan el ancho de banda al que transmiten los clientes en color azul, y el ancho de banda que dichos clientes obtienen en color verde; y en forma de **tablas** donde se miden dichos anchos de banda y los paquetes descartados. Las gráficas se obtienen usando el **programa generador** de tráfico *Traffic Generator* [21] instalado en los PCs clientes y servidor. Las tablas se obtienen del *router* a través de la aplicación *Hyperterminal* introduciendo el comando:

 # show ip traffic-filter stats

Previamente a cada simulación se deben resetear los resultados de las tablas mediante el comando:

 # config ip traffic-filter clear-stats

La **duración de las pruebas es de 120 segundos**, tiempo que se considera suficiente como para que los estadísticos proporcionen resultados veraces.

El fin último del proyecto es estudiar la QoS en situación de **congestión**. El ancho de banda del **enlace final** es de **10 Mbps**, por tanto, la suma de los contratos de los cuatro clientes no debe superar este valor. Así, en la configuración "Mismo Contrato", a cada cliente se le asigna un contrato de 2 Mbps, dando un total de **8 Mbps de ancho de banda contratado**, con lo que sobran 2 Mbps (ancho de banda en exceso) que las herramientas *DiffServ* deben repartir de manera "**equitativa"** entre los clientes. Este reparto, del ancho de banda no contratado, dependerá del escenario configurado y es el que **se analizará** en los casos que se exponen.

En la configuración "Distintos Contratos", al igual que en "Mismo Contrato", se desea que la suma de los contratos asignados dé un ancho de banda total contratado de 8 Mbps; de este modo, los 2 Mbps que sobran, se espera que las herramientas *DiffServ* lo distribuyan entre los clientes de manera **"proporcional"** a la tasa contratada. En la tabla 3.11 se muestran el identificador del filtro que se corresponde con cada cliente, las tasas asignadas (distintos contratos) a cada cliente y el valor al que equivalen para introducirlo en la configuración.

Los puertos de entrada a los que llegan sus respectivos flujos de tráfico se configuran como nodos frontera (*access port*) para que así, tenga lugar:

- el **acondicionamiento del tráfico** mediante funciones policía (con *Token Buckets*) y comprobar si los flujos de tráfico cumplen sus contratos,
- el **marcado DSCP** (los paquetes que cumplan el contrato serán marcados con un DSCP y aquellos cuya tasa supere lo contratado se marcarán con un DSCP distinto)
- y la **clasificación de los paquetes**.

En ellos se lleva a cabo todas las funciones necesarias para implementar *DiffServ*, en concreto el servicio ***Assured Forwarding***. Concretamente las clases de servicio Plata y Oro.

Las fuentes C3 y C4 entregan tráfico a las interfaces del *switch BPS 2000* (puertos 17 y 24 respectivamente) y las fuentes C1 y C2 entregan tráfico a las interfaces del router *Passport 8600 Routing Switch* (puertos 45 y 25, respectivamente). El tráfico total sale de la interfaz del *router* correspondiente al puerto 15 donde se provocará la situación de congestión.

Tabla 3.11: Tasas contratadas para la configuración "Distintos Contratos" TCP>UDP

Id Filtro	**Clientes**	**Contrato**	**Valores "AverageRate"**
1	C1	1,4 M	27
3	C3	1,8 M	34
		3,2 M	
		40% de 8 M 32% de 10 M	
2	C2	2,2 M	42
4	C4	2,6 M	50
		4,8M	
		60% de 8 M 48% de 10M	
Ancho de Banda Total Contratado		8 M	
Ancho de Banda del enlace final		10 M	
Ancho de Banda en exceso (no contratado)		**2 M**	

Las políticas de QoS aplicadas a cada flujo generado por su respectivo cliente, marcará todos los paquetes:

a) conformes con el contrato (In-Profile):

1) con el DSCP 18 = '010**01**0'= 12 hex = AF21

si los paquetes son asignados a la Cola 3 = Clase de Servicio Plata.

2) con el DSCP 26 = '011**01**0' = 1A hex = AF31

si los paquetes son asignados a la Cola 4 = Clase de Servicio Oro.

Nota: Los bits en negrita '**01**' indican el nivel bajo en la precedencia de descarte de los paquetes.

b) que excedan su respectivo contrato (Out-Profile):

1) con el DSCP 20 = '010**10**0' = 14 hex = AF22

si los paquetes son asignados a la Cola 3 = Clase de Servicio Plata.

2) con el DSCP 28 = '011**10**0' = 1C hex = AF32

si los paquetes son asignados a la Cola 4 = Clase de Servicio Oro.

Nota: Los bits en negrita '**10**' indican el nivel medio en la precedencia de descarte de los paquetes.

A continuación, se exponen los resultados obtenidos:

3.3.3.1 Caso Plata: configuración con una cola

3.3.3.1.1 Sin aplicar Servicios Diferenciados (sin activar DROP)

a. Mismo contrato

i. Tráfico generado TCP: todas las fuentes son TCP y tienen el mismo contrato.

1. Tráfico generado por cada cliente: 1,25 Mbps

Tráfico total generado: 1,25 * 4 = 5 Mbps, 50% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

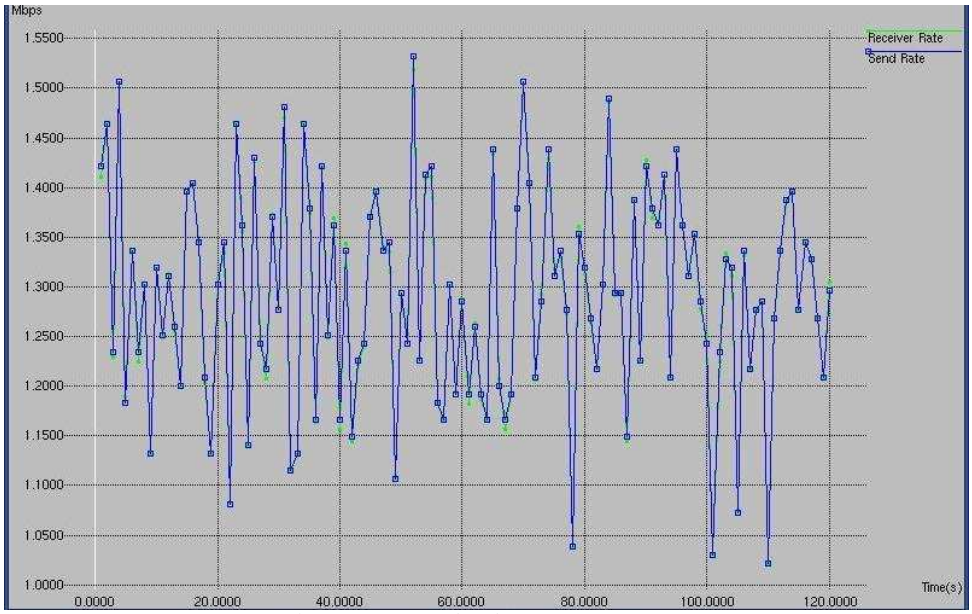


Figura 3.6: C1 (2M) PLATA a 1,25M

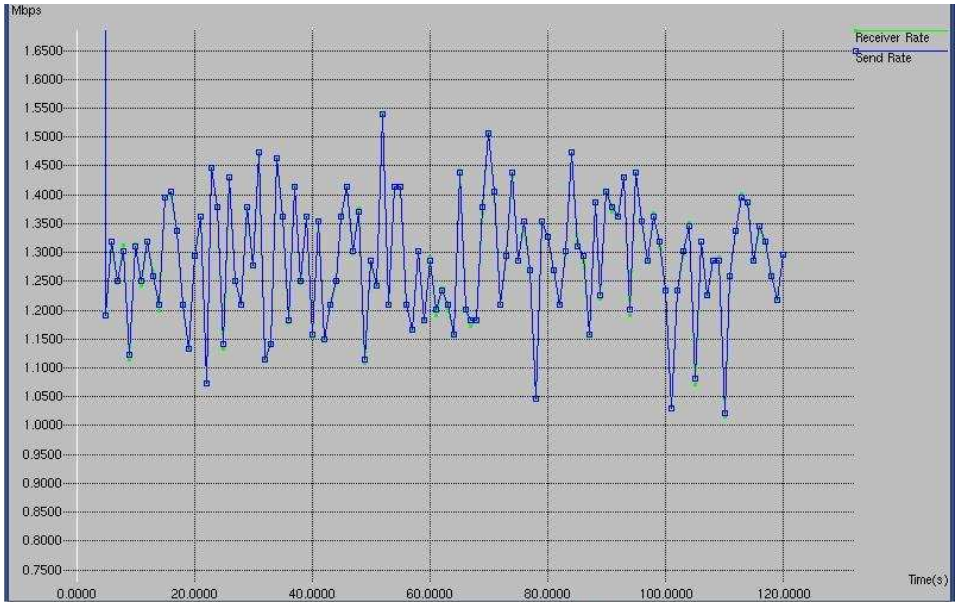


Figura 3.7: C2 (2M) PLATA a 1,25M

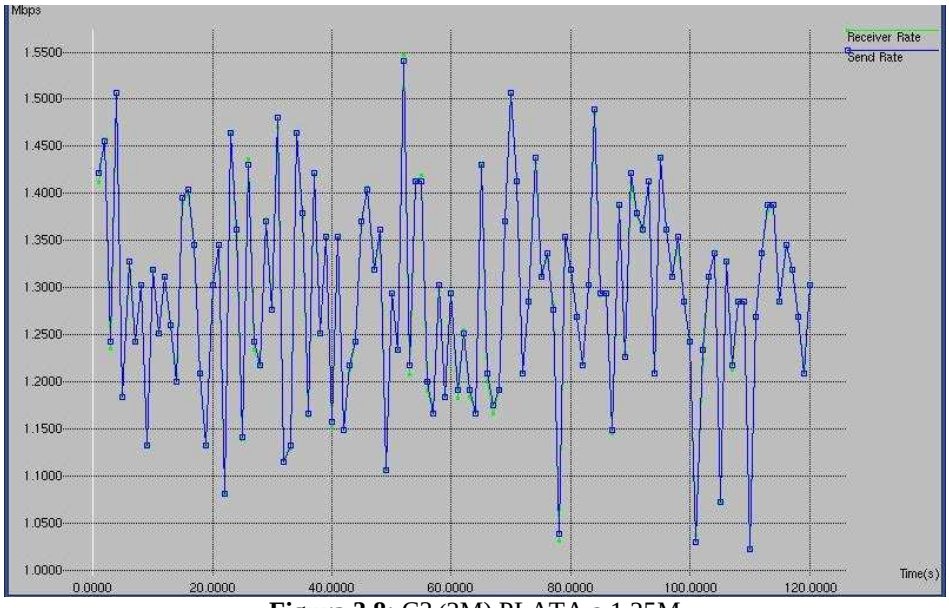


Figura 3.8: C3 (2M) PLATA a 1,25M

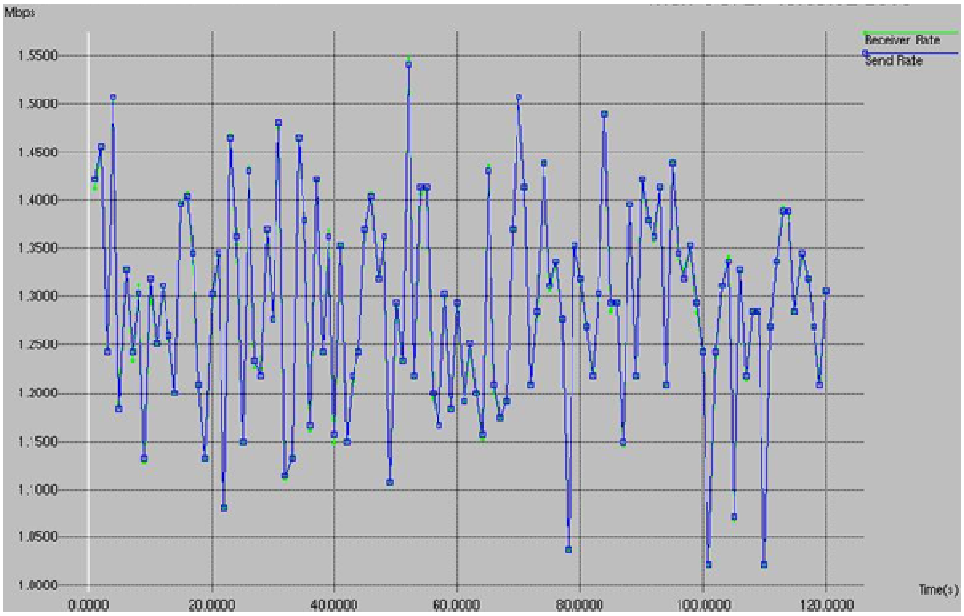


Figura 3.9: C4 (2M) PLATA a 1,25M

En todas las gráficas se observa que la línea azul coincide con la línea verde, con lo cual todos los clientes obtienen el ancho de banda al que transmiten.

En la tabla de resultados 3.12, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.12: Resultados para todas las fuentes TCP a 1,25M "Mismo Contrato" 2M

Filter ID	Filter- PKTS	Filter-OCTETS	TRAFFIC PROFILE DISCARD PKTS	BW (Mbps)
1	17738	19872324	0	**1,324821**
3	17639	19865394	0	**1,324359**
4	17701	19869734	0	**1,324648**
2	17546	19858892	0	**1,323926**

Todos los clientes obtienen el mismo ancho de banda.
Al tratarse de **sólo tráfico TCP** y **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **1,32M**. Este valor no coincide con el configurado 1,25M ya que el programa generador de tráfico *Traffic Generator* genera en media.

2. **Tráfico generado por cada cliente: 2 Mbps**

   Tráfico total generado: 2 * 4 = 8 Mbps, 80% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

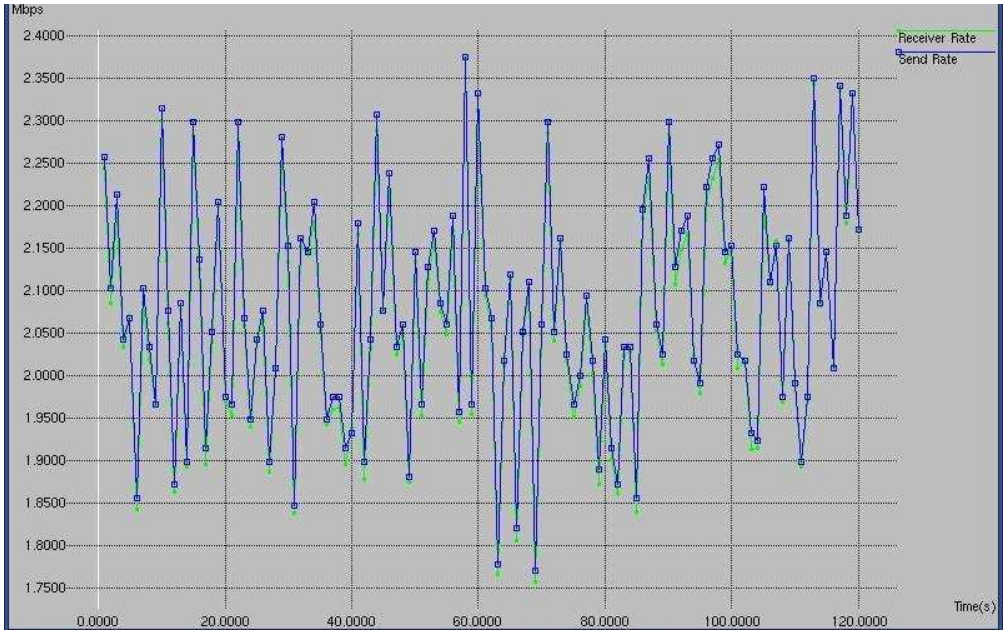


Figura 3.10: C1 (2M) PLATA a 2M

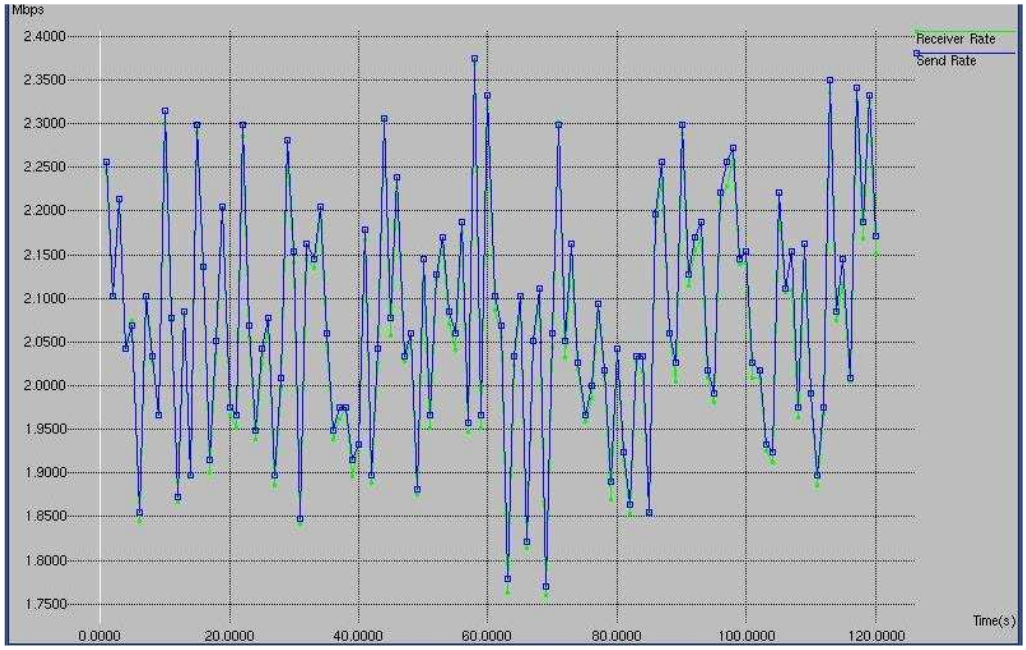


Figura 3.11: C2 (2M) PLATA a 2M

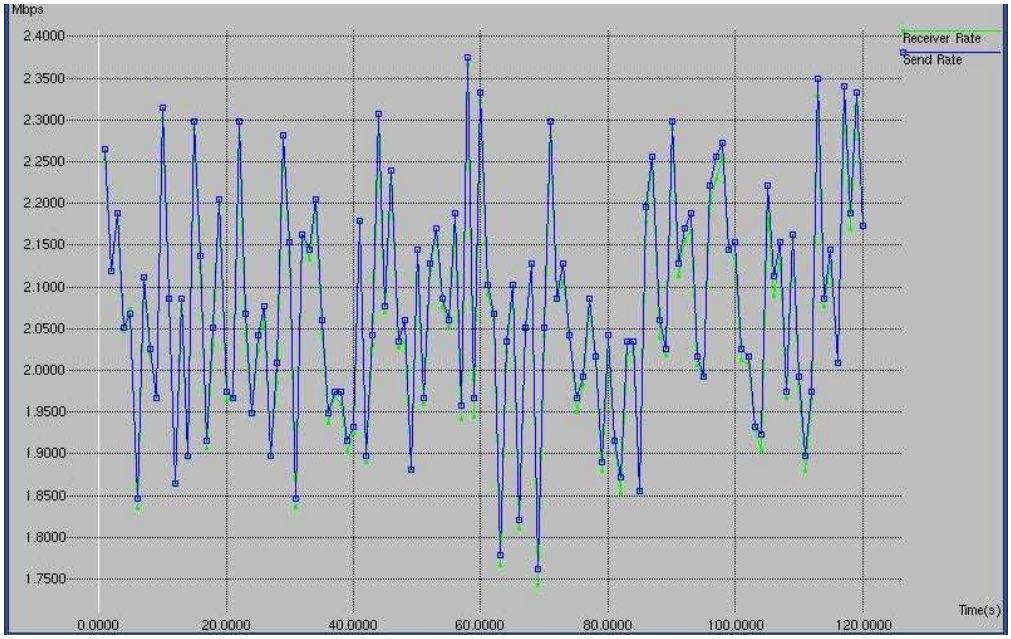


Figura 3.12: C3 (2M) PLATA a 2M

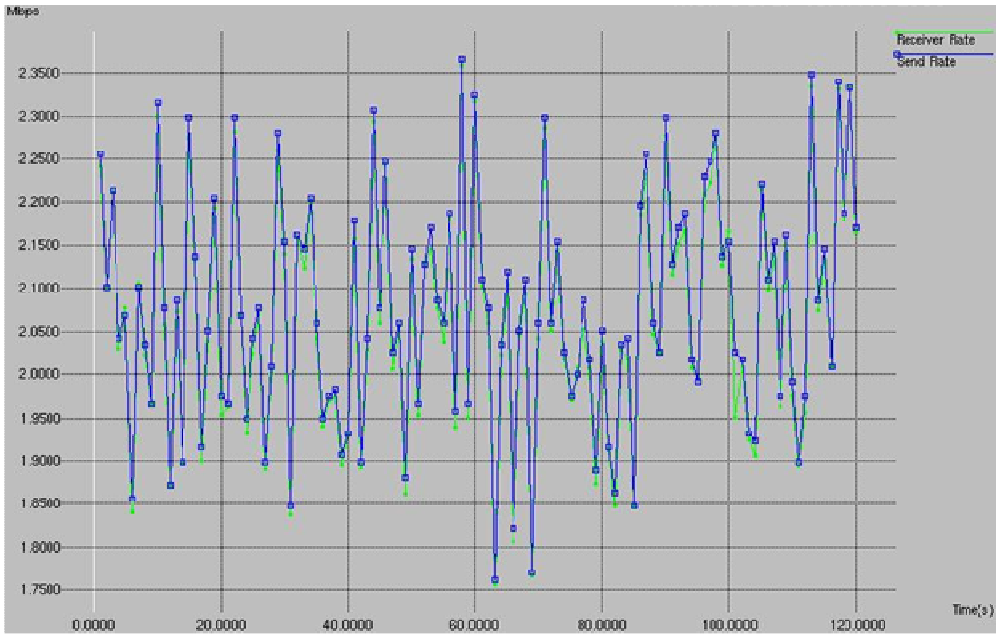


Figura 3.13: C4 (2M) PLATA a 2M

En todas las gráficas se observa que la línea azul prácticamente coincide con la línea verde, con lo cual todos los clientes obtienen el ancho de banda al que transmiten.

En la tabla de resultados 3.13, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.13: Resultados para todas las fuentes TCP a 2M "Mismo Contrato" 2M

Filter ID	Filter- PKTS	Filter-OCTETS	TRAFFIC PROFILE DISCARD PKTS	BW (Mbps)
1	25462	31738444	0	**2,11589**
3	25315	31728154	0	**2,11521**
4	25285	31726054	0	**2,11507**
2	25332	31729344	0	**2,11528**

Todos los clientes obtienen el mismo ancho de banda.
Al tratarse de **sólo tráfico TCP** y **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **2,11M**.

Nota: Se debe tener en cuenta que el programa generador de tráfico *Traffic Generator* genera en media.

3. Tráfico generado por cada cliente: 3 Mbps

Tráfico total generado: 3 * 4 = 12 Mbps, 120% del ancho de banda total. Por tanto, se forma **cuello de botella en** el enlace final.

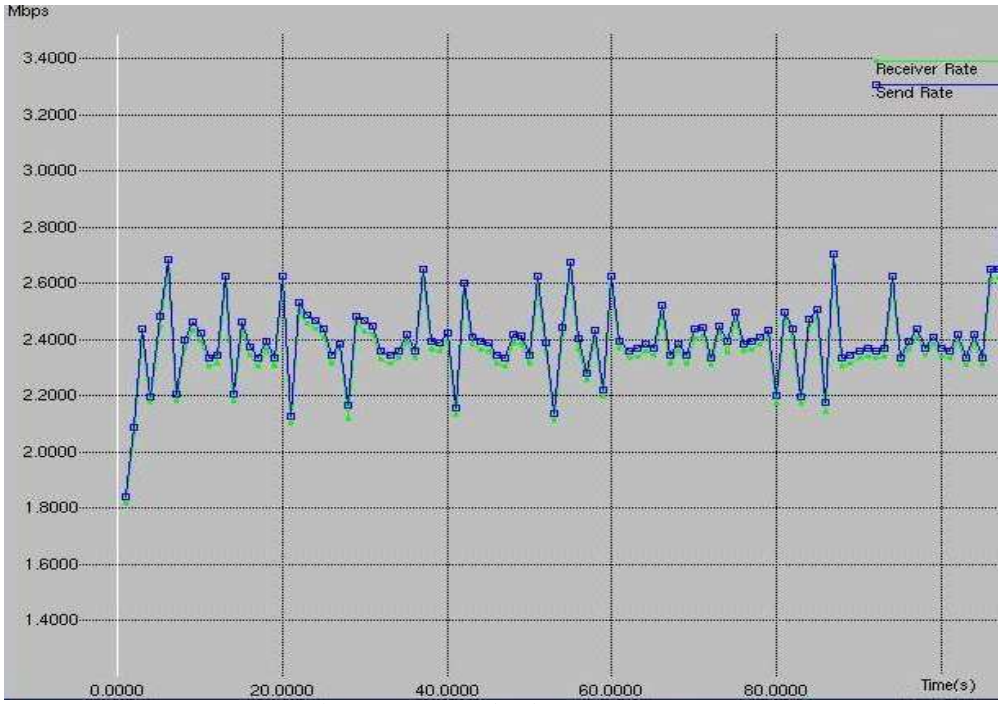


Figura 3.14: C1 (2M) PLATA a 3M

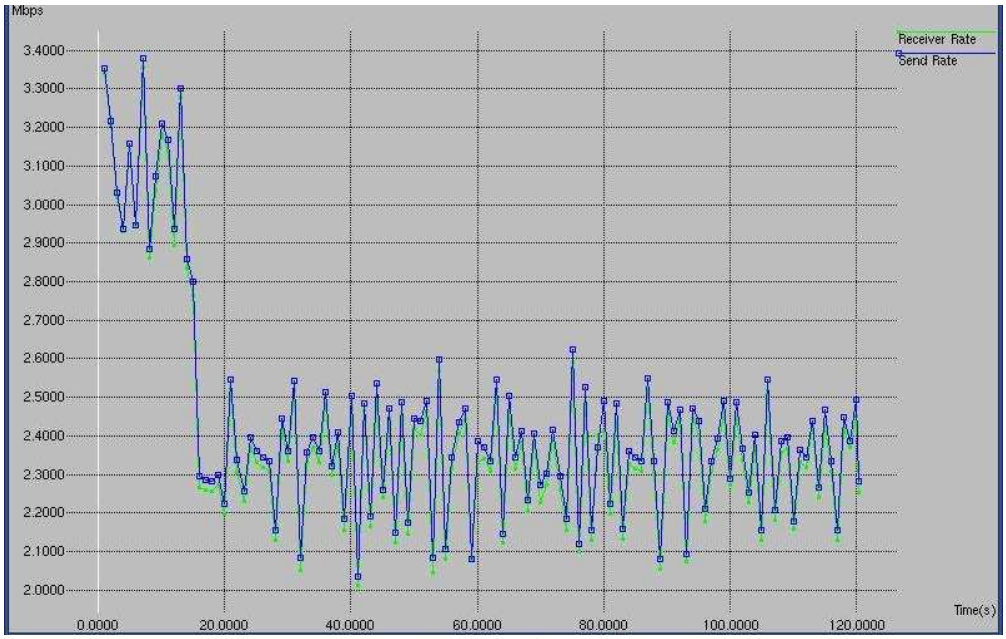


Figura 3.15: C2 (2M) PLATA a 3M

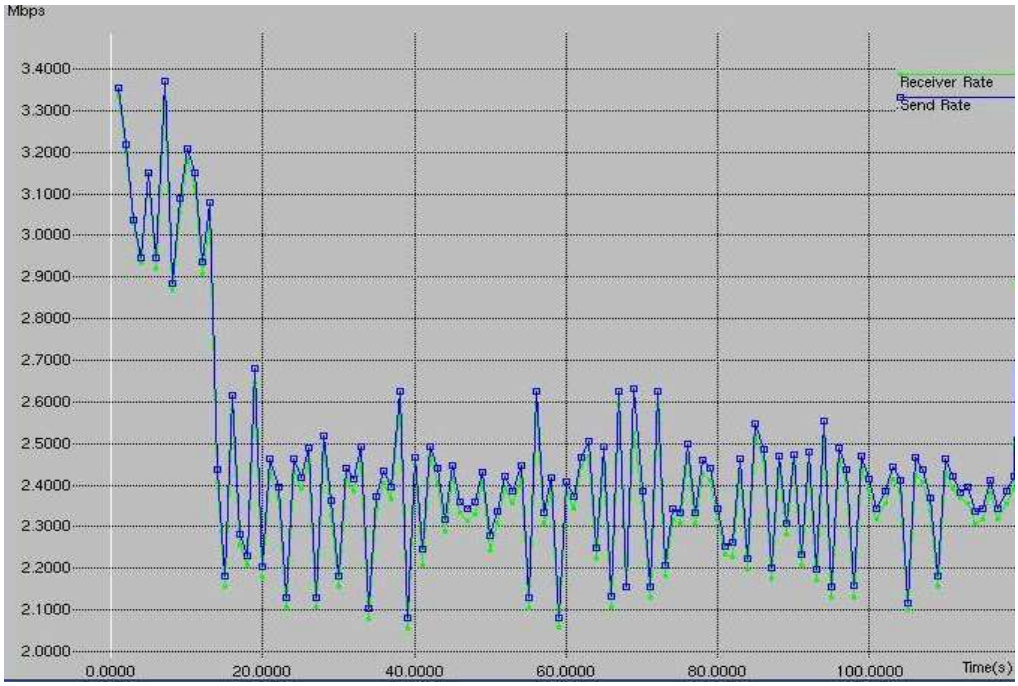


Figura 3.16: C3 (2M) PLATA a 3M

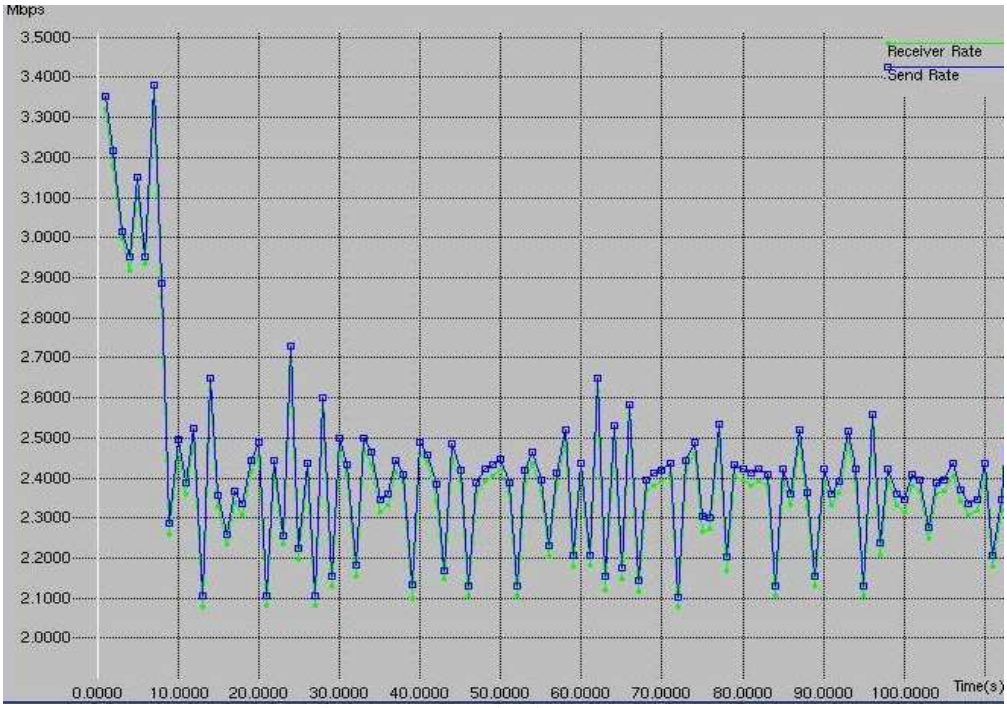


Figura 3.17: C4 (2M) PLATA a 3M

En todas las gráficas se observa que la línea azul queda ligeramente por encima de la línea verde, ya que en este caso al estar en **situación de congestión** y ser todas las fuentes TCP, los clientes no obtienen el ancho de banda al que transmiten tráfico.
Cada cliente puede obtener como máximo 10/4 = 2,5M del ancho de banda total. Se reparte los 10M del enlace final entre los cuatro clientes TCP, equitativamente. Se observa como en un principio todos los clientes comienzan a generar a 3M hasta detectar la congestión. Señalar que en la gráfica del cliente C1, al empezar a transmitir más tarde, directamente transmite a la ventana de transmisión (2,5M en media) que le corresponde en esta situación de congestión.
Cada cliente no obtiene los 3M de ancho de banda a los genera tráfico, sino que al **detectar congestión** reducen su ventana de transmisión, llevándose por tanto 2,5M (en media) del canal, esto es, aproximadamente la cuarta parte de los 10M del canal.

En la tabla de resultados 3.14, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.14: Resultados para todas las fuentes TCP a 3M "Mismo Contrato" 2M

Filter ID	Filter- PKTS	Filter-OCTETS	TRAFFIC PROFILE DISCARD PKTS	BW (Mbps)
1	25473	37445880	0	**2,496392**
3	25491	37492410	0	**2,499494**
4	25561	37595025	0	**2,506335**
2	25474	37466685	0	**2,497779**

Se observa cómo prácticamente se obtiene el mismo ancho de banda, 2,5M para todos los clientes.

ii. Tráfico generado UDP y TCP

1. Tráfico generado por cada cliente: 1,25 Mbps

Tráfico total generado: 1,25 * 4 = 5 Mbps, 50% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

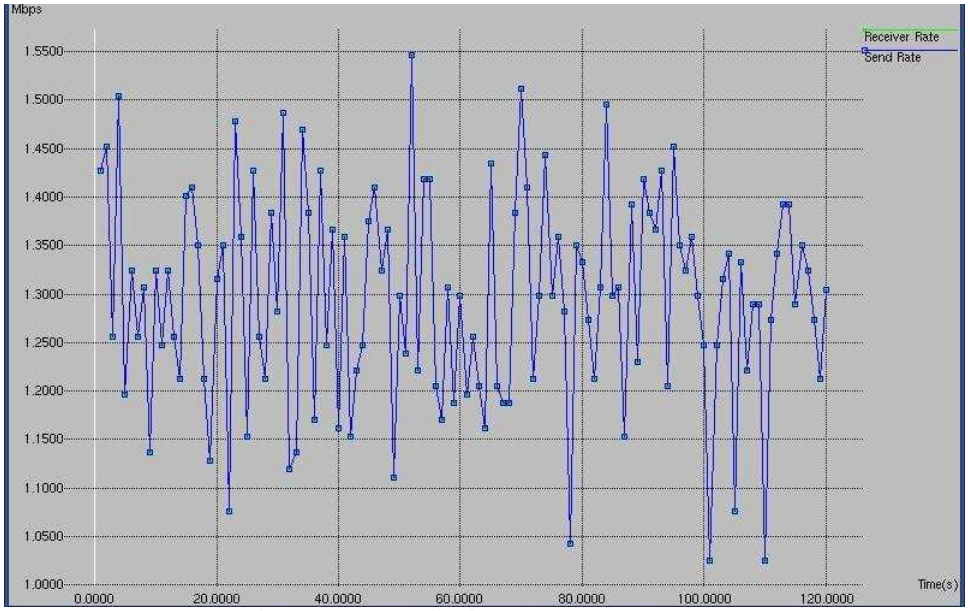


Figura 3.18: C1 (2M) UDP PLATA a 1,25M

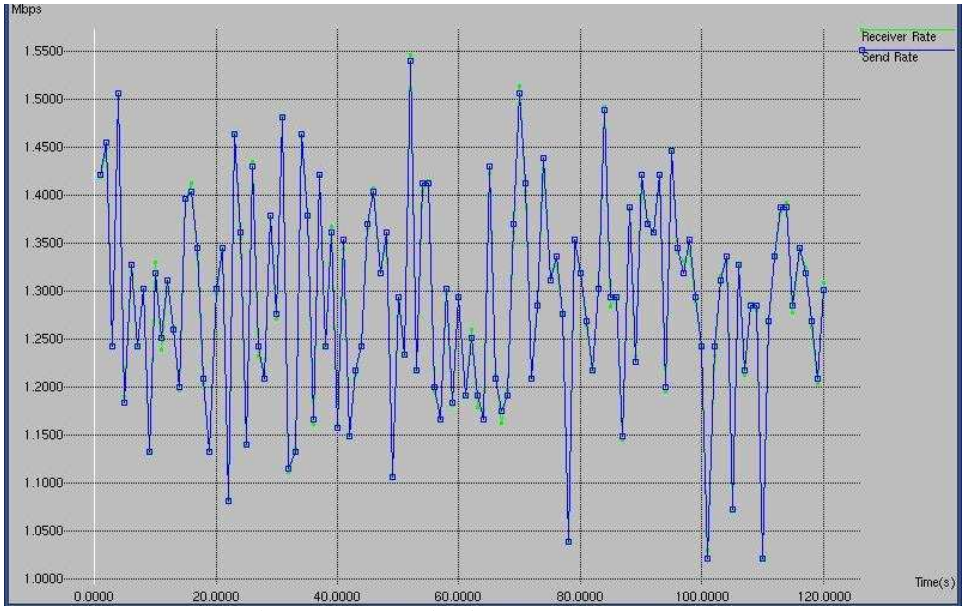


Figura 3.19: C2 (2M) TCP PLATA a 1,25M

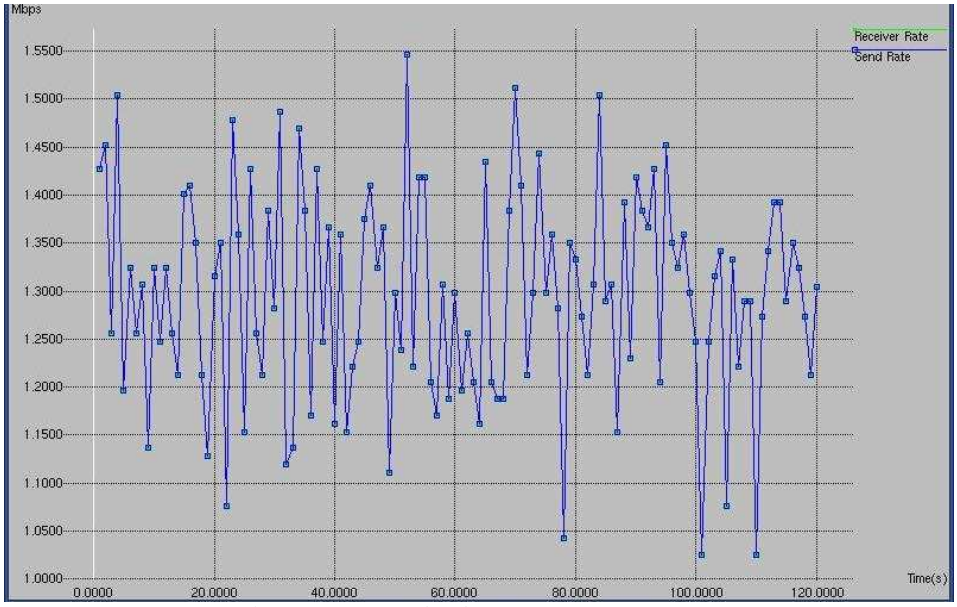


Figura 3.20: C3 (2M) UDP PLATA a 1,25M

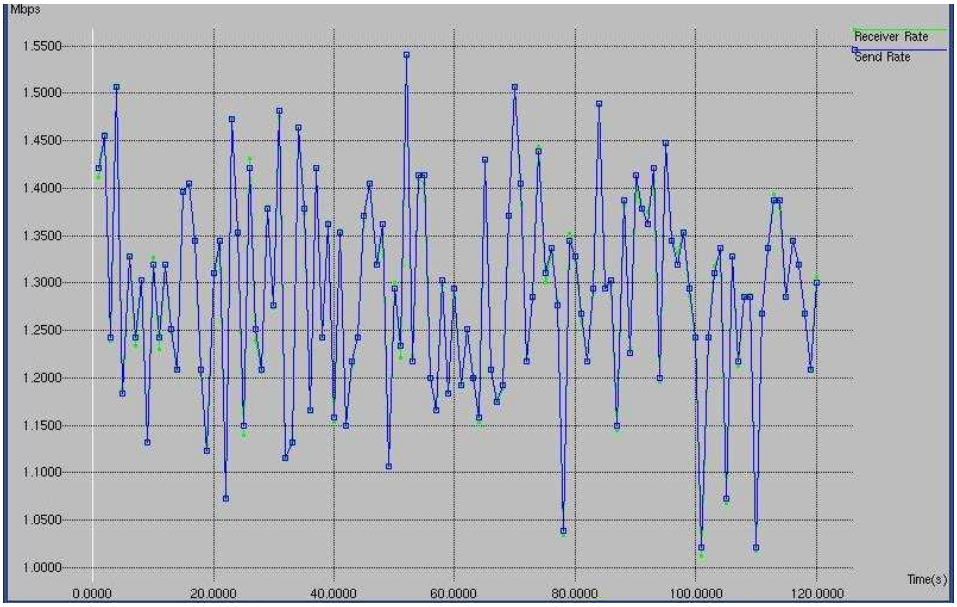


Figura 3.21: C4 (2M) TCP PLATA a 1,25M

En todas las gráficas se observa que la línea azul coincide con la línea verde, con lo cual todos los clientes obtienen el ancho de banda al que transmiten.

En la tabla de resultados 3.15, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.15: Resultados para fuentes UDP y TCP a 1,25M "Mismo Contrato" 2M

Filter ID	Filter- PKTS	Filter-OCTETS	TRAFFIC PROFILE DISCARD PKTS	BW (Mbps)
UDP				
1	18194	19540356	0	**1,30269**
3	18194	19540356	0	**1,30269**
TCP				
4	17641	19865534	0	**1,324368**
2	17723	19871274	0	**1,324751**

Todos los clientes obtienen el mismo ancho de banda.
Al **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **1,3M**.

Nota: Se debe tener en cuenta que el programa generador de tráfico *Traffic Generator* genera en media.

2. Tráfico generado por cada cliente: 2 Mbps

Tráfico total generado: 2 * 4 = 8 Mbps, 80% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

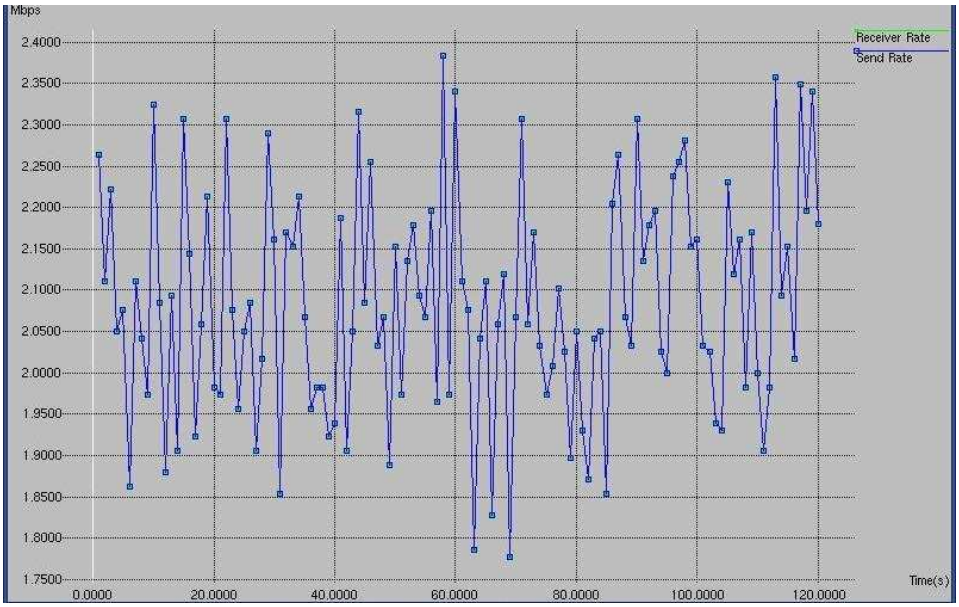


Figura 3.22: C1 (2M) UDP PLATA a 2M

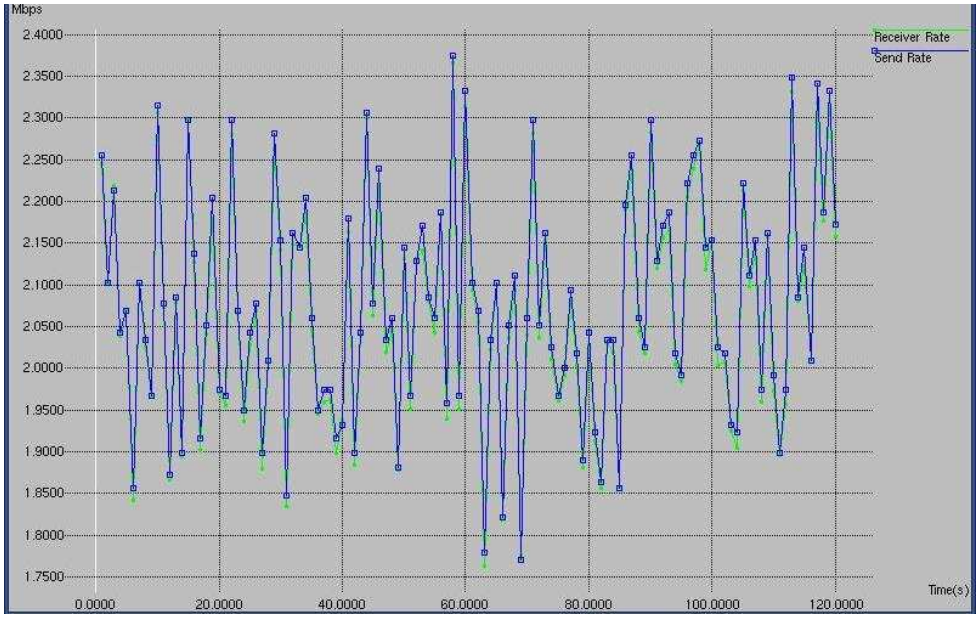


Figura 3.23: C2 (2M) TCP PLATA a 2M

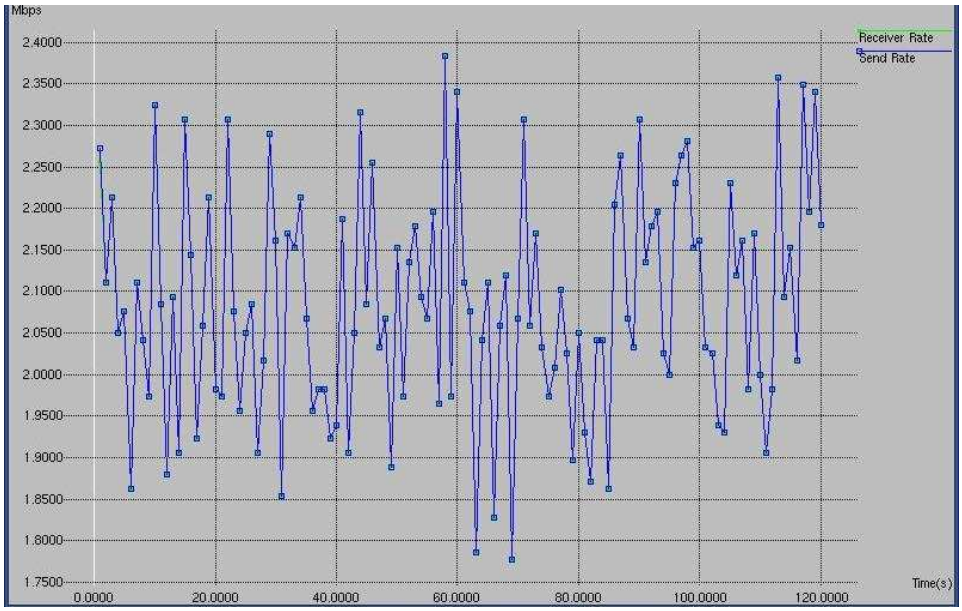


Figura 3.24: C3 (2M) UDP PLATA a 2M

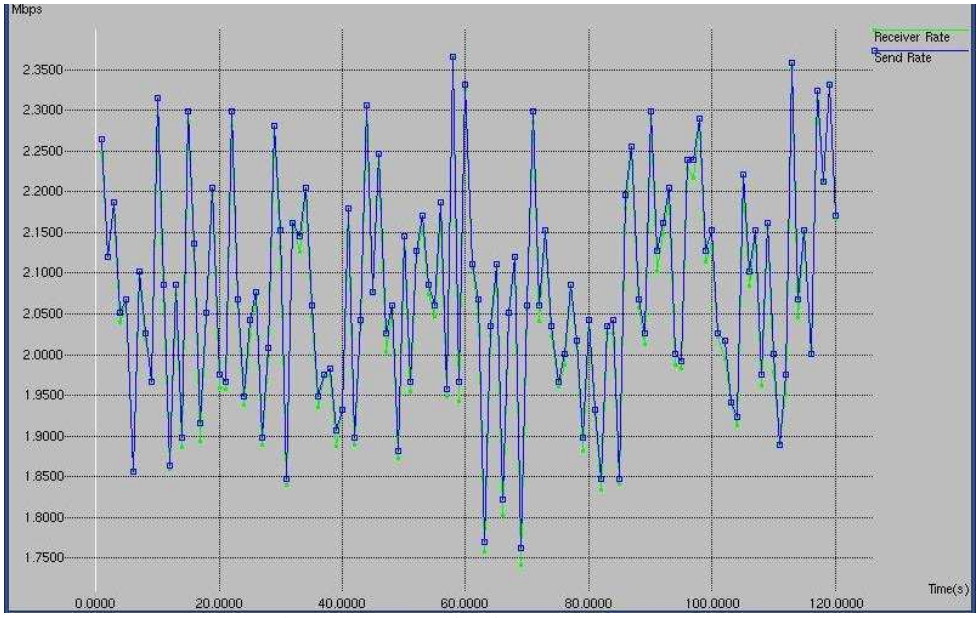


Figura 3.25: C4 (2M) TCP PLATA a 2M

En este escenario se ocupa el 80% del canal, con lo cual se está en el límite a partir del cual las prestaciones de la red comienzan a degradarse. Pasado este límite el tráfico **UDP acapara los recursos de la red frente al tráfico TCP.**
Se observa, por un lado, que en las gráficas de tráfico UDP, clientes C1 y C3, **la línea azul coincide perfectamente con la línea verde**, es decir, transmiten a la tasa máxima, con lo cual los clientes UDP obtienen el ancho de banda al que transmiten.
Por otro lado, en las gráficas de tráfico TCP, clientes C2 y C4 se aprecia que la línea azul prácticamente coincide con la línea verde, con lo cual se puede decir que los clientes TCP obtienen el ancho de banda al que transmiten. La diferencia con las gráficas de tráfico UDP, es que en las de tráfico TCP se distinguen picos verdes ligeramente por debajo de la línea azul, esto es debido a que se genera tráfico en media y cuando se enfrenta tráfico UDP frente a TCP, el **UDP no colabora**, es decir, **no reduce su ventana de transmisión** y continúa transmitiendo a la tasa máxima.

En la tabla de resultados 3.16, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.16: Resultados para fuentes UDP y TCP a 2M "Mismo Contrato" 2M

Filter ID	Filter- PKTS	Filter-OCTETS	TRAFFIC PROFILE DISCARD PKTS	BW (Mbps)
UDP				
1	29254	31418796	0	**2,094586**
3	29252	31416648	0	**2,094443**
TCP				
4	25185	31719054	0	**2,114603**
2	25246	31724348	0	**2,114956**

Todos los clientes obtienen el mismo ancho de banda.
Al **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **2,1M**.

Nota: Se debe tener en cuenta que el programa generador de tráfico *Traffic Generator* genera en media.

3. Tráfico generado por cada cliente: 3 Mbps

Tráfico total generado: 3 * 4 = 12 Mbps, 120% del ancho de banda total. Por tanto, se forma **cuello de botella en** el enlace final.

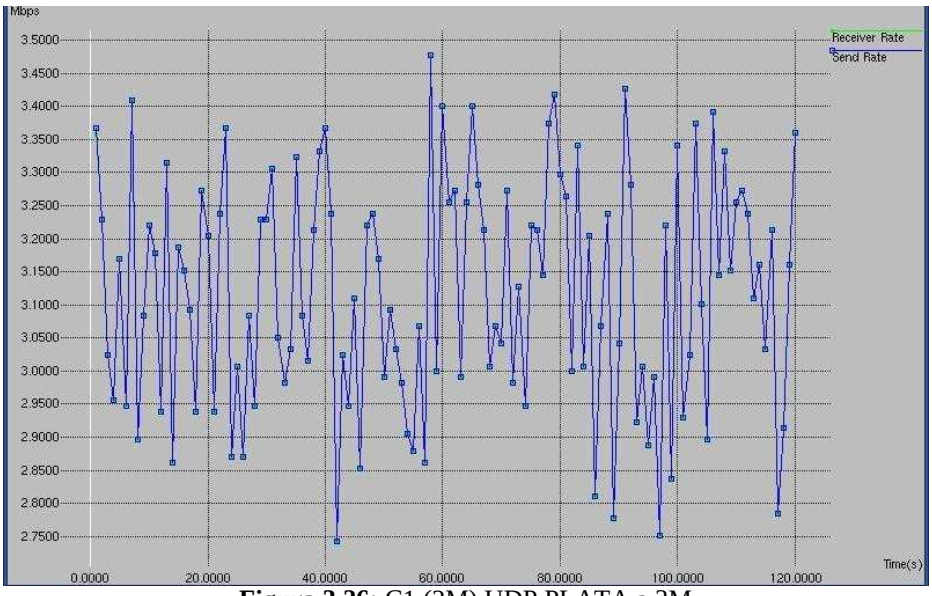


Figura 3.26: C1 (2M) UDP PLATA a 3M

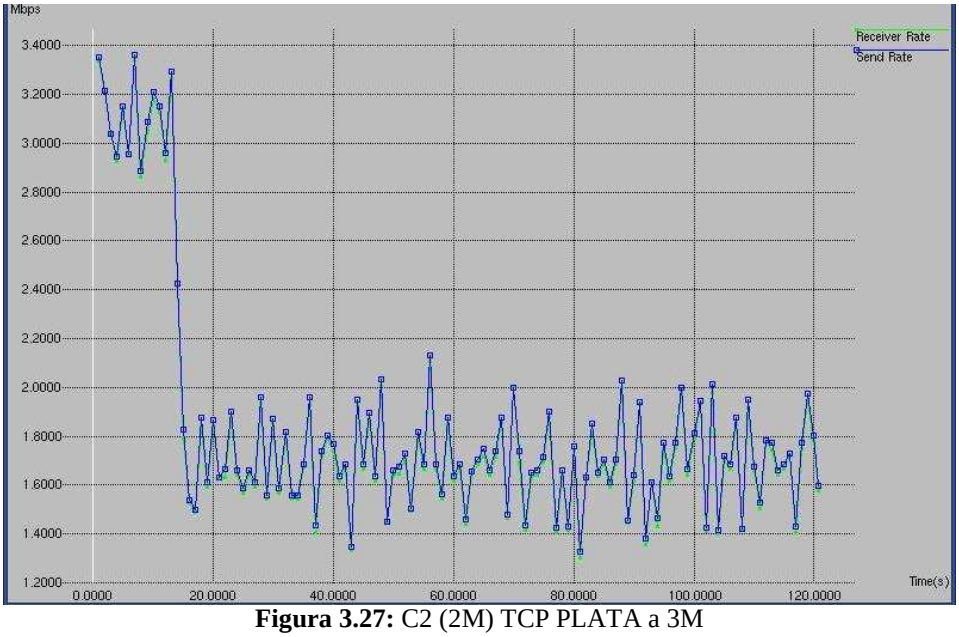


Figura 3.27: C2 (2M) TCP PLATA a 3M

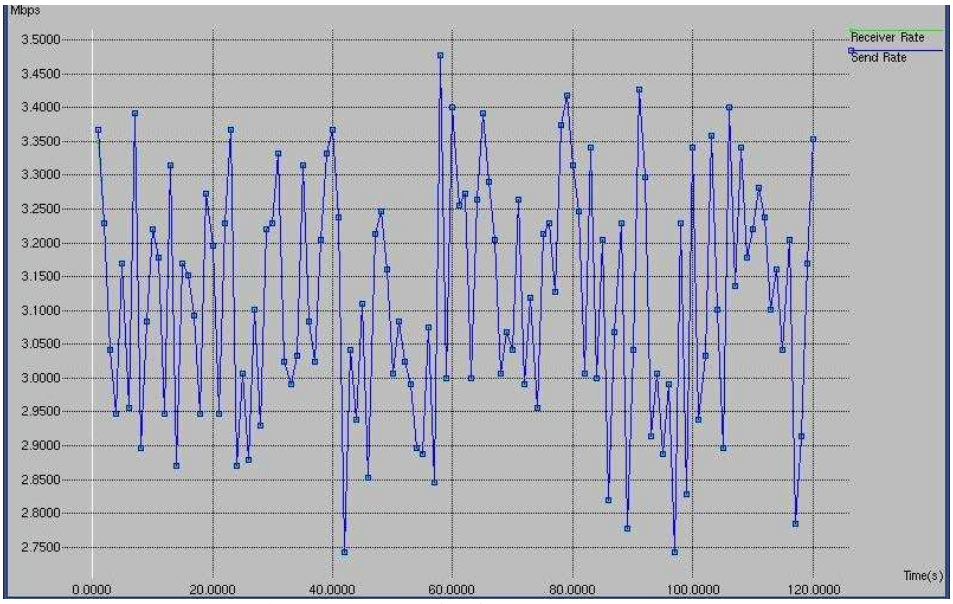


Figura 3.28: C3 (2M) UDP PLATA a 3M

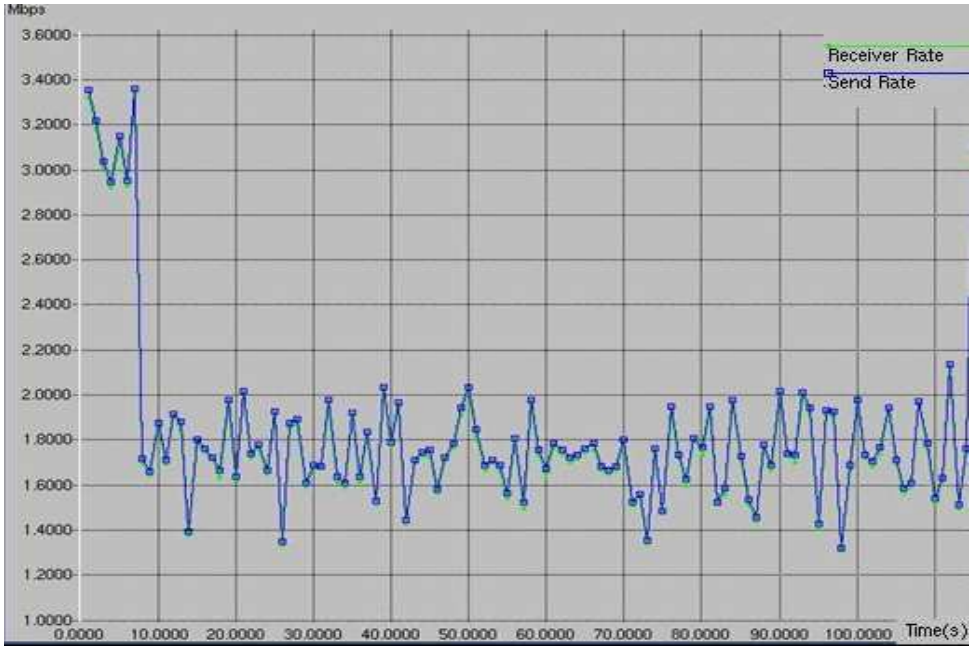


Figura 3.29: C4 (2M) TCP PLATA a 3M

En las gráficas de tráfico TCP, clientes C2 y C4, se observa que la línea azul queda ligeramente por encima de la línea verde, ya que en este caso al estar en **situación de congestión** las fuentes TCP no obtienen el ancho de banda máximo al que transmiten.
Se observa como en un principio los **clientes TCP** comienzan a generar tráfico a 3M hasta detectar la congestión. En ese momento, los clientes TCP no obtiene los 3M de ancho de banda a los genera tráfico, ya que al **detectar congestión** reducen su ventana de transmisión.
Los **clientes UDP**, clientes C1 y C3, consiguen los 3M a los que generan tráfico, puesto que las fuentes UDP no se enteran de la congestión y continuarán transmitiendo a la tasa máxima. Del ancho de banda total sobran 2M para cada cliente TCP.

En la tabla de resultados 3.17, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.17: Resultados para fuentes UDP y TCP a 3M "Mismo Contrato" 2M

Filter ID	Filter- PKTS	Filter-OCTETS	TRAFFIC PROFILE DISCARD PKTS	BW (Mbps)
UDP				
1	43795	47035830	0	**3,13572**
3	43794	47034756	0	**3,13565**
TCP				
4	19422	28220250	0	**1,88135**
2	19462	28283908	0	**1,88559**

Por un lado, los **clientes TCP**, C2 y C4, obtienen un ancho de banda cercano a 2M (**1,88M**), ya que reducen su ventana de transmisión al detectar congestión. Por otro lado, los **clientes UDP**, C1 y C3, obtienen **3,13M** consiguiendo el ancho de banda al que generan tráfico, por tratarse de tráfico UDP. La suma da 10M que es el total del ancho de banda del enlace. Al estar en situación de congestión, el tráfico UDP va a conseguir el ancho de banda al que genera tráfico, es decir, los clientes C1 y C3 consiguen un total de aproximadamente 6M del ancho de banda total, quedando alrededor de 4M a repartir entre los clientes C2 y C4. Al generar éstos tráfico TCP, y estar en situación de congestión, TCP avisa que se **disminuya la tasa de generación de paquetes**, optando cada cliente a conseguir en torno a 2M del ancho de banda del enlace final.

b. Distintos contratos

i. Tráfico generado TCP: todas las fuentes son TCP y tienen distintos contratos.

En esta prueba, los contratos de las fuentes TCP C2 y C4 son mayores que los contratos de las fuentes TCP C1 y C3.

1. **Tráfico generado por cada cliente: 1,25 Mbps**

   Tráfico total generado: 1,25 * 4 = 5 Mbps, 50% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

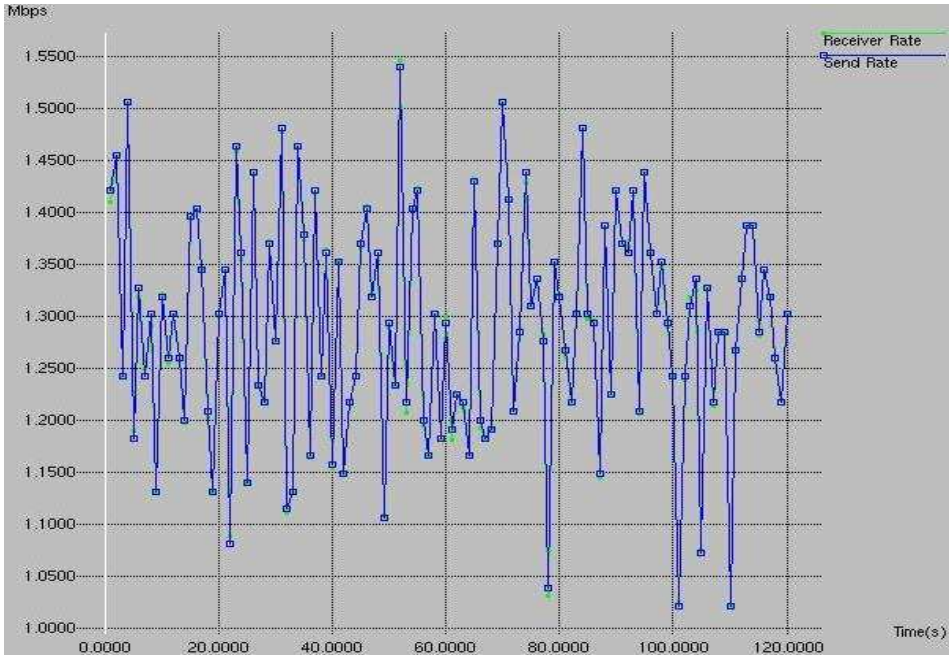


Figura 3.30: C1 (1,4M) PLATA a 1,25M

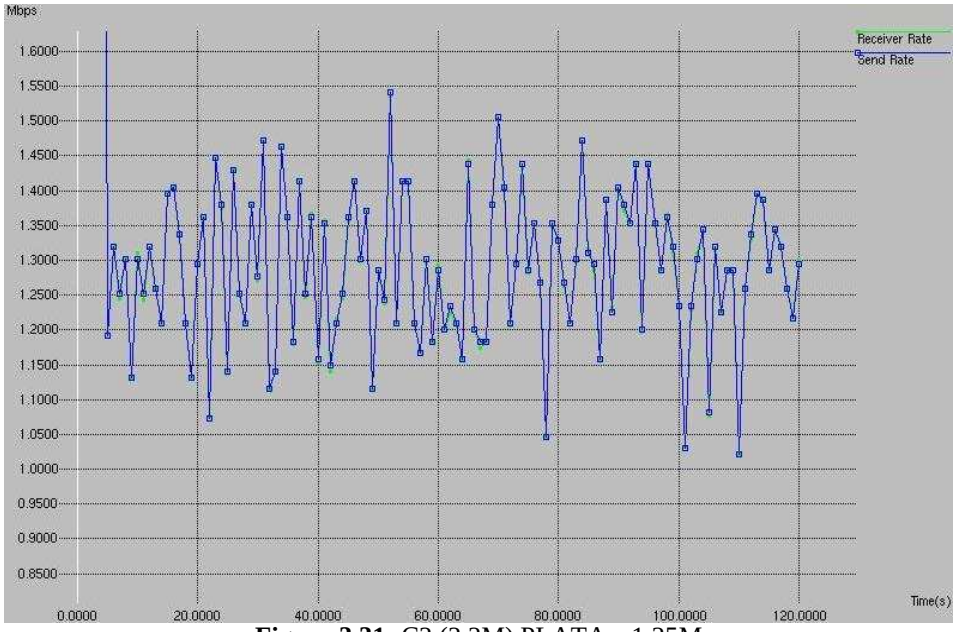


Figura 3.31: C2 (2,2M) PLATA a 1,25M

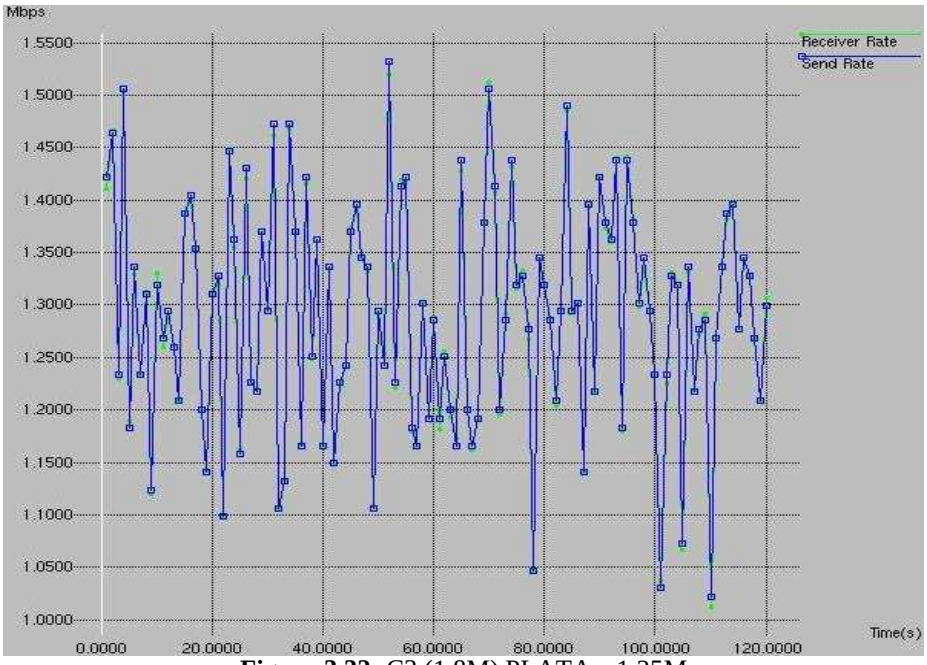


Figura 3.32: C3 (1,8M) PLATA a 1,25M

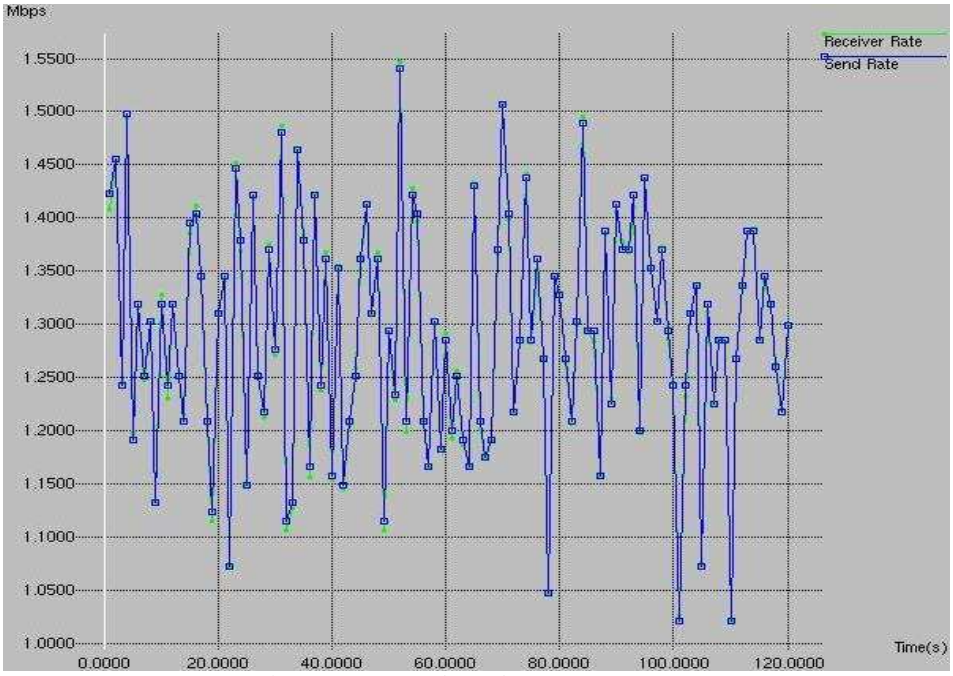


Figura 3.33: C4 (2,6M) PLATA a 1,25M

En todas las gráficas se observa que la línea azul coincide con la línea verde, con lo cual todos los clientes obtienen el ancho de banda al que transmiten.

En la tabla de resultados 3.18, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.18: Resultados para todas las fuentes TCP a 1,25M "Distintos Contratos"

Filter ID	Filter- PKTS	Filter-OCTETS	TRAFFIC PROFILE DISCARD PKTS	BW (Mbps)
1 (1,4M)	17783	19875474	0	**1,325031**
3 (1,8M)	17725	19871414	0	**1,324760**
4 (2,6M)	17707	19870166	0	**1,324677**
2 (2,2M)	17598	19862532	0	**1,324168**

Todos los clientes obtienen el mismo ancho de banda.
Al tratarse de **sólo tráfico TCP** y **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **1,32M**.

Nota: el programa generador *Traffic Generator* genera tráfico en media.

2. Tráfico generado por cada cliente: 2 Mbps

Tráfico total generado: 2 * 4 = 8 Mbps, 80% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

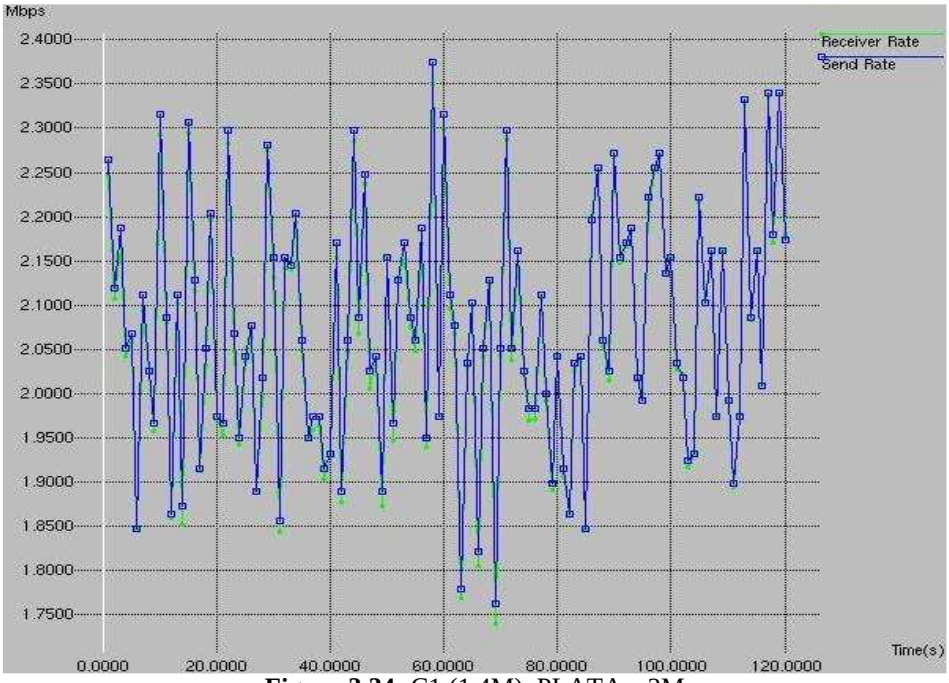


Figura 3.34: C1 (1,4M) PLATA a 2M

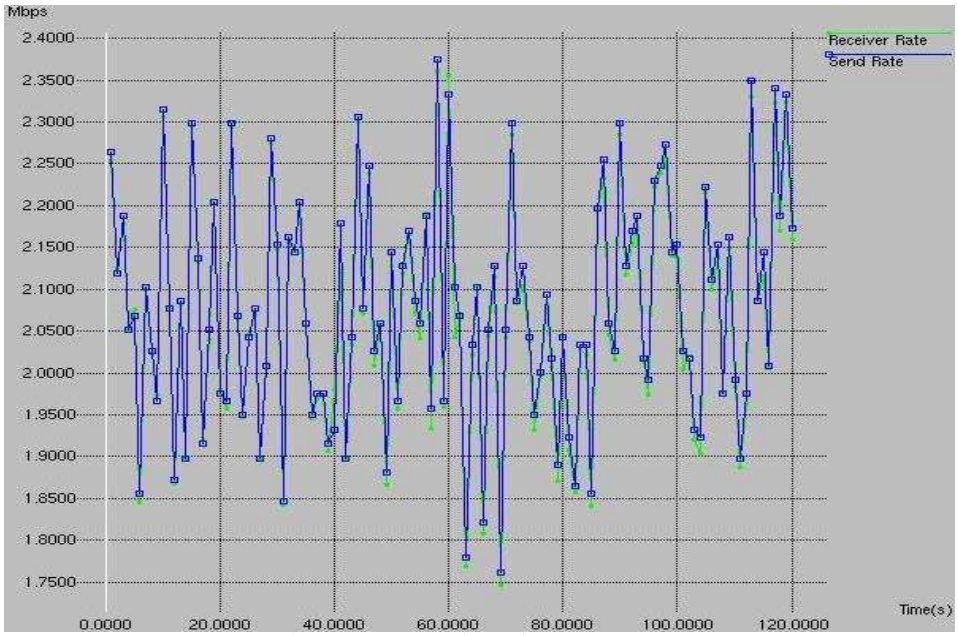


Figura 3.35: C2 (2,2M) PLATA a 2M

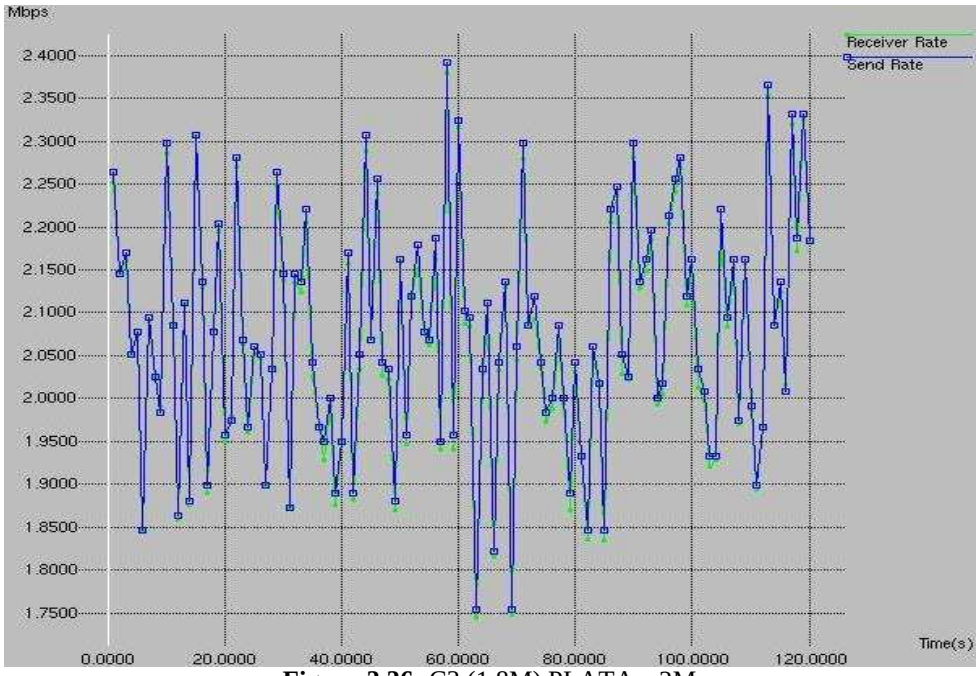


Figura 3.36: C3 (1,8M) PLATA a 2M

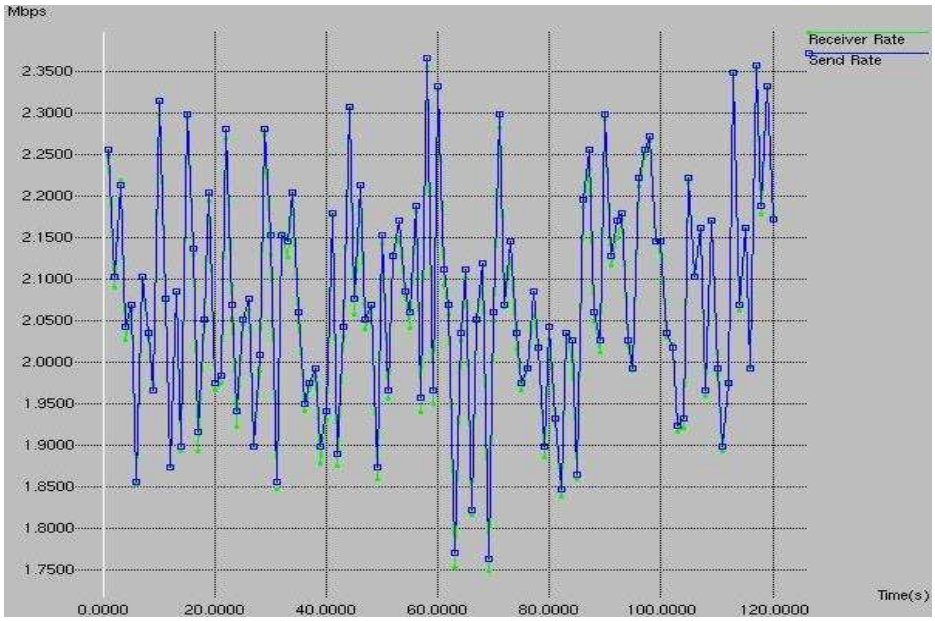


Figura 3.37: C4 (2,6M) PLATA a 2M

En todas las gráficas se observa que la línea azul prácticamente coincide con la línea verde, con lo cual todos los clientes obtienen el ancho de banda al que transmiten.

En la tabla de resultados 3.19, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.19: Resultados para todas las fuentes TCP a 2M "Distintos Contratos"

Filter ID	Filter- PKTS	Filter-OCTETS	TRAFFIC PROFILE DISCARD PKTS	BW (Mbps)
1 (1,4M)	26181	31788774	0	**2,119251**
3 (1,8M)	25962	31933444	0	**2,128896**
4 (2,6M)	23568	31606568	0	**2,107104**
2 (2,2M)	26149	31786534	0	**2,119102**

Todos los clientes obtienen el mismo ancho de banda.
Al tratarse de **sólo tráfico TCP** y **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **2,1M**.

Nota: el programa generador *Traffic Generator* genera tráfico en media.

3. **Tráfico generado por cada cliente: 3 Mbps**

   Tráfico total generado: 3 * 4 = 12 Mbps, 120% del ancho de banda total. Por tanto, se forma **cuello de botella en** el enlace final.

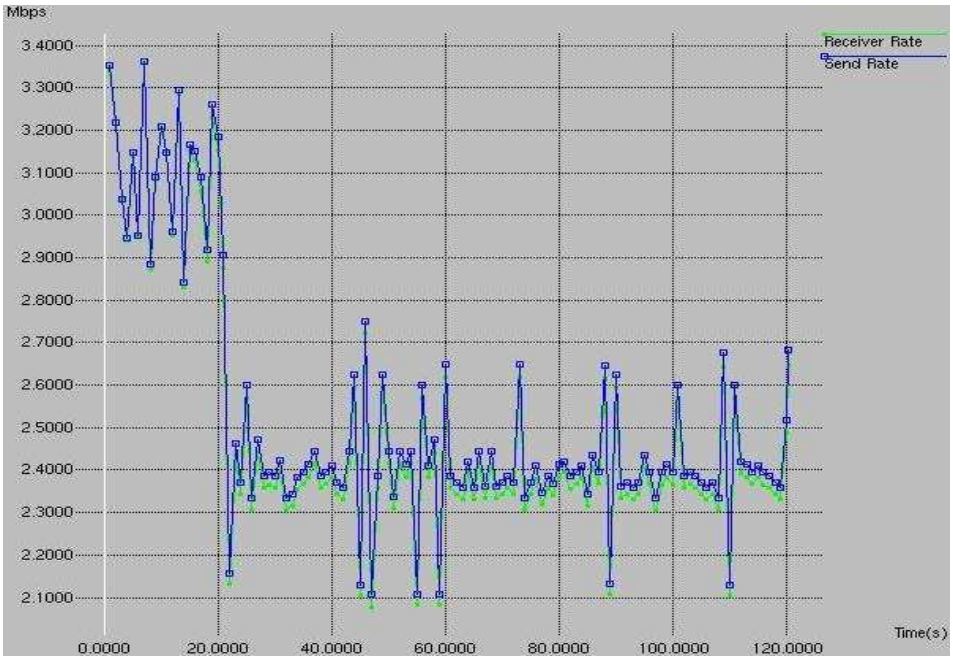


Figura 3.38: C1 (1,4M) PLATA a 3M

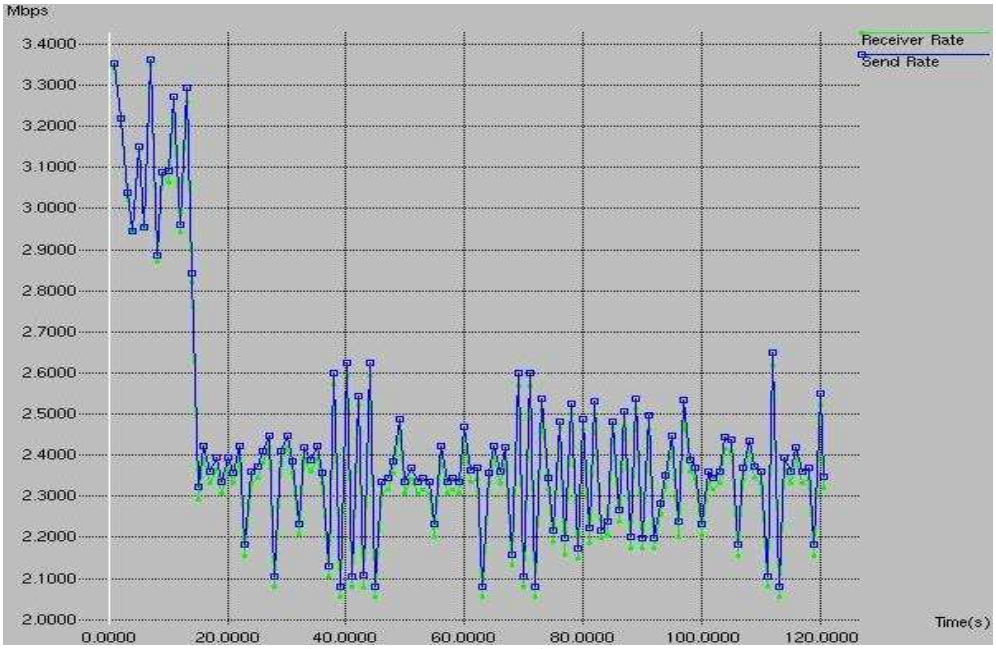


Figura 3.39: C2 (2,2M) PLATA a 3M

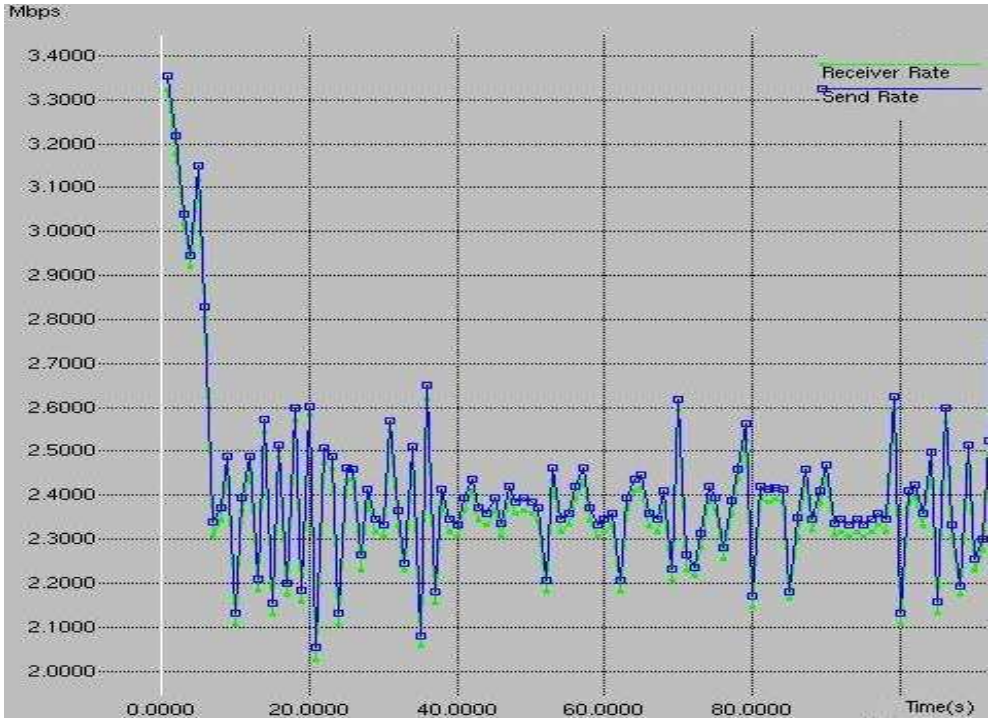


Figura 3.40: C3 (1,8M) PLATA a 3M

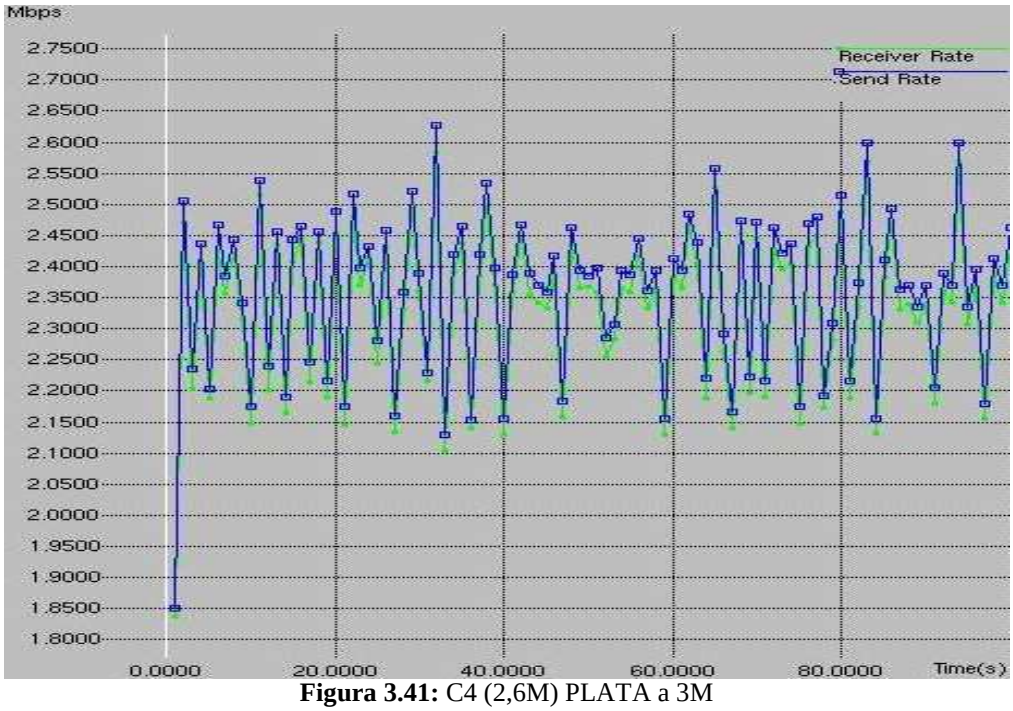


Figura 3.41: C4 (2,6M) PLATA a 3M

En todas las gráficas se observa que la línea azul queda ligeramente por encima de la línea verde, ya que en este caso al estar en **situación de congestión** y ser todas las fuentes TCP, los clientes no obtienen el ancho de banda al que transmiten.

Cada cliente puede obtener como máximo 10/4 = 2,5M del ancho de banda total. Se reparten los 10M del enlace final entre los cuatro clientes TCP, equitativamente. Se observa como en un principio todos los clientes comienzan a generar a 3M hasta detectar la congestión. Señalar que en la gráfica del cliente C4, al empezar a transmitir más tarde, directamente transmite a la ventana de transmisión (2,5M en media) que le corresponde en esta situación de congestión. Cada cliente no obtiene los 3M de ancho de banda a los genera tráfico, sino que al **detectar congestión** reducen su ventana de transmisión, llevándose por tanto 2,5M (en media) del canal, esto es, aproximadamente la cuarta parte de los 10M del canal.

En la tabla de resultados 3.20, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.20: Resultados para todas las fuentes TCP a 3M "Distintos Contratos"

Filter ID	Filter- PKTS	Filter-OCTETS	TRAFFIC PROFILE DISCARD PKTS	BW (Mbps)
1 (1,4M)	25559	37736714	0	**2,51578**
3 (1,8M)	25451	37989378	0	**2,53262**
4 (2,6M)	25624	37214130	0	**2,48094**
2 (2,2M)	25543	37095786	0	**2,47305**

Se observa cómo prácticamente se obtiene el mismo ancho de banda 2,5M para todos los clientes.

ii. Tráfico generado UDP y TCP

En esta prueba, los **contratos** de las fuentes generadoras de tráfico **TCP** C2 y C4 son **mayores** que los contratos de las fuentes generadoras de tráfico **UDP** C1 y C3.

1. Tráfico generado por cada cliente: 1,25 Mbps

Tráfico total generado: 1,25 * 4 = 5 Mbps, 50% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

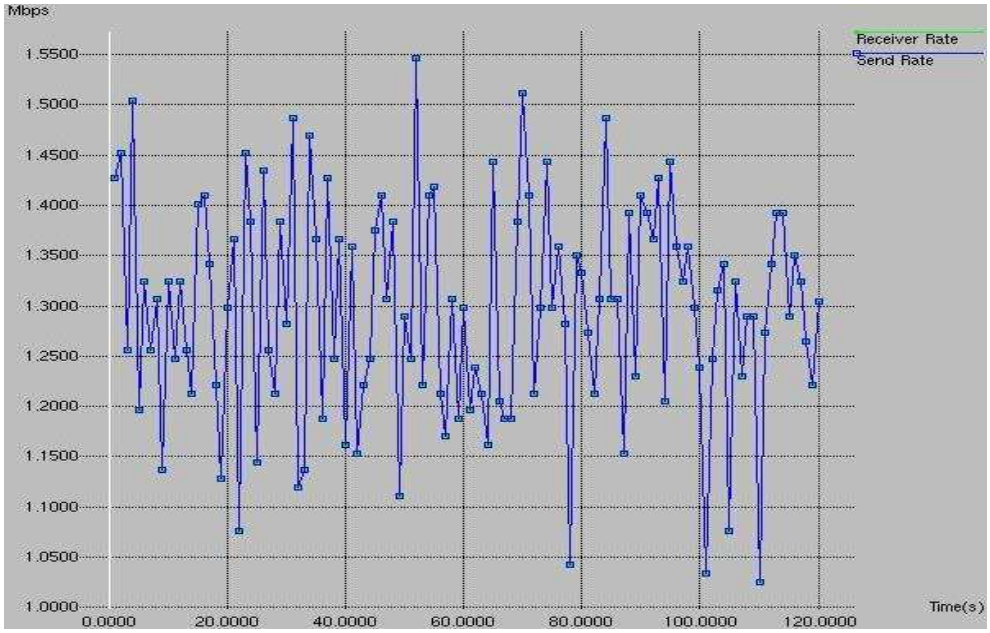


Figura 3.42: C1 (1,4M) UDP PLATA a 1,25M

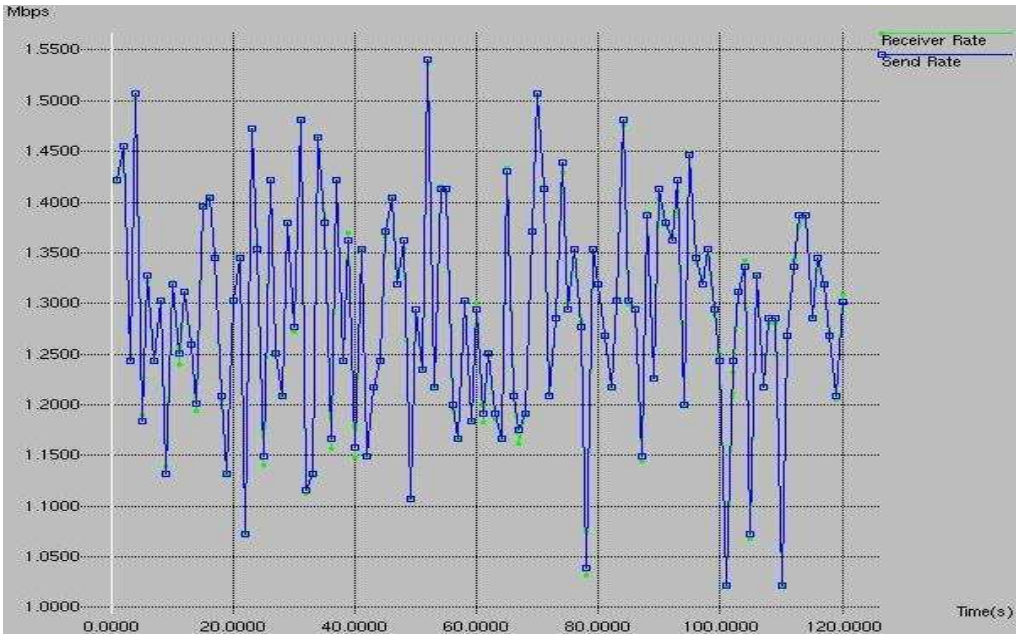


Figura 3.43: C2 (2,2M) TCP PLATA a 1,25M

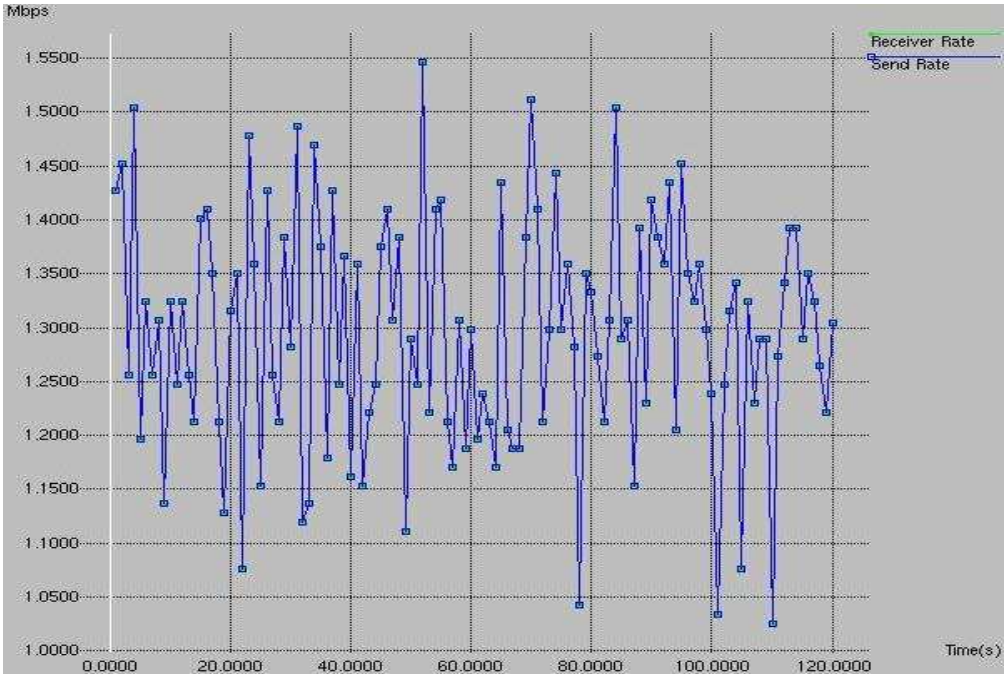


Figura 3.44: C3 (1,8M) UDP PLATA a 1,25M

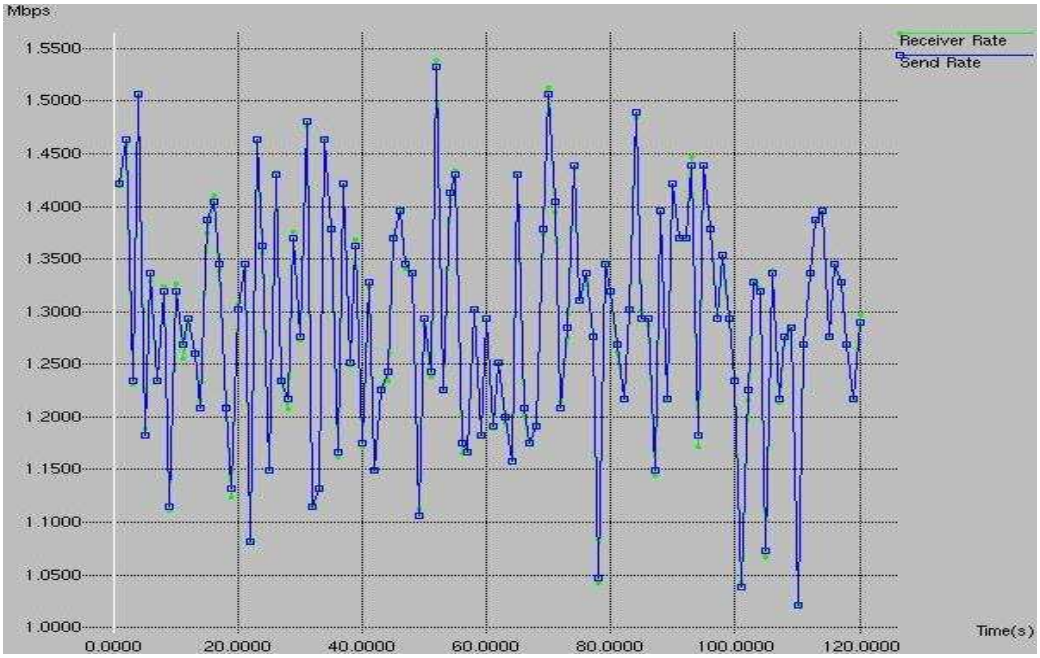


Figura 3.45: C4 (2,6M) TCP PLATA a 1,25M

En todas las gráficas se observa que la línea azul coincide con la línea verde, con lo cual todos los clientes obtienen el ancho de banda al que transmiten.

En la tabla de resultados 3.21, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.21: Resultados para fuentes UDP y TCP a 1,25M "Distintos Contratos"

Filter ID	Filter- PKTS	Filter-OCTETS	TRAFFIC PROFILE DISCARD PKTS	BW (Mbps)
UDP				
1 (1,4M)	18194	19540356	0	**1,30269**
3 (1,8M)	18194	19540356	0	**1,30269**
TCP				
4 (2,6M)	17664	19867144	0	**1,324476**
2 (2,2M)	17752	19873304	0	**1,324886**

Todos los clientes obtienen el mismo ancho de banda.
Al **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **1,3M**.

Nota: el programa generador *Traffic Generator* genera tráfico en media.

2. **Tráfico generado por cada cliente: 2 Mbps**

   Tráfico total generado: 2 * 4 = 8 Mbps, 80% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

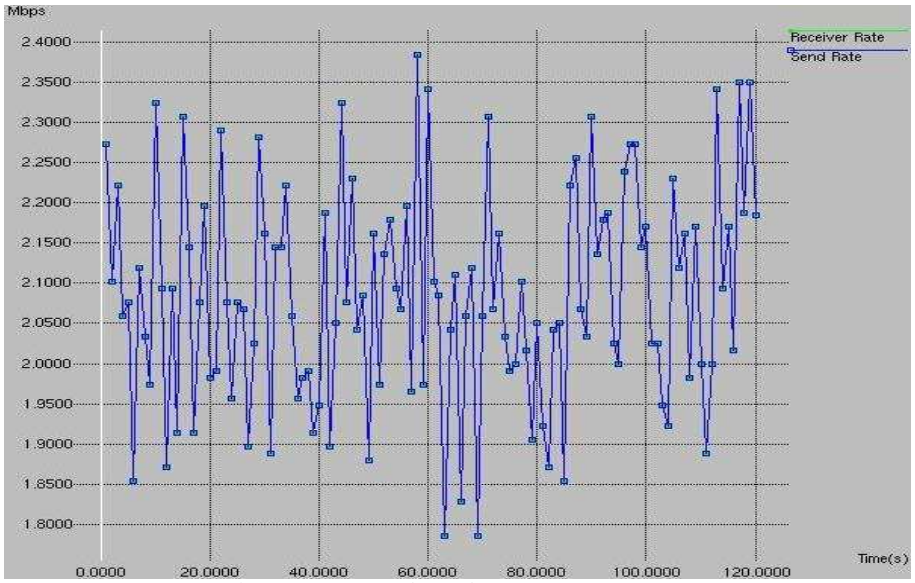


Figura 3.46: C1 (1,4M) UDP PLATA a 2M

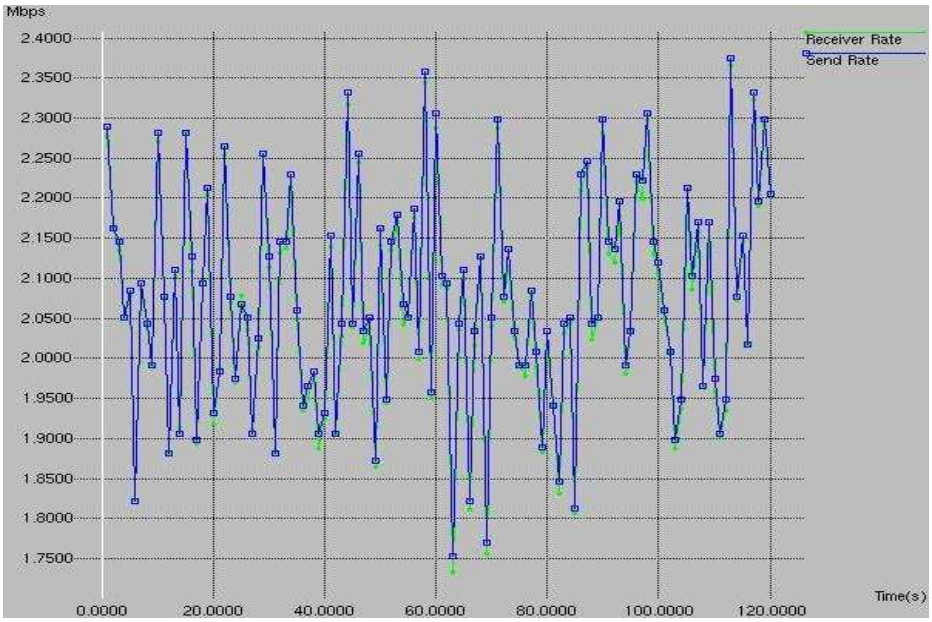


Figura 3.47: C2 (2,2M) TCP PLATA a 2M

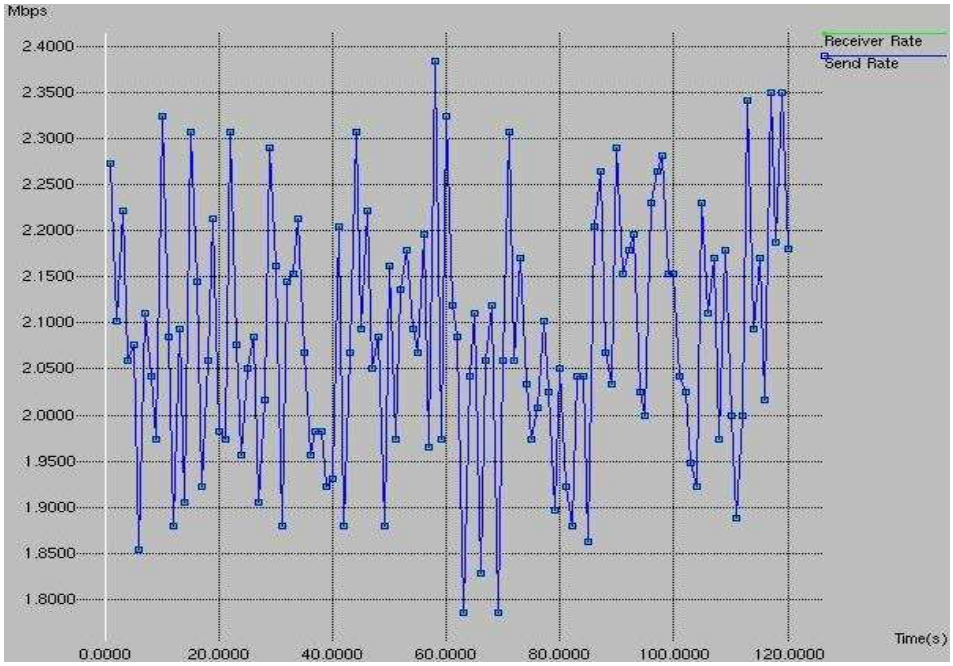


Figura 3.48: C3 (1,8M) UDP PLATA a 2M

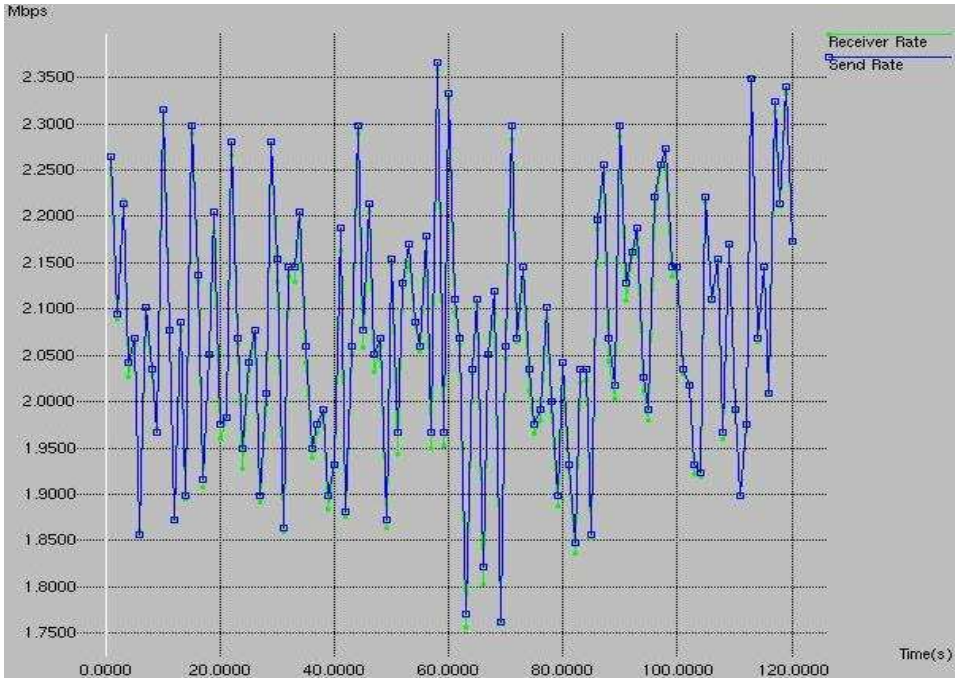


Figura 3.49: C4 (2,6M) TCP PLATA a 2M

En este escenario se ocupa el 80% del canal, con lo cual se está en el límite a partir del cual las prestaciones de la red comienzan a degradarse. Pasado este límite el tráfico UDP acapara los recursos de red frente al tráfico TCP.

Por un lado, se observa que en las gráficas de tráfico UDP, clientes C1 y C3, la línea azul coincide perfectamente con la línea verde, es decir, transmiten a la tasa máxima, con lo cual los clientes UDP obtienen el ancho de banda al que transmiten.

Por otro lado, en las gráficas de tráfico TCP, clientes C2 y C4 se aprecia que la línea azul prácticamente coincide con la línea verde, con lo cual se puede decir que los clientes TCP obtienen el ancho de banda al que transmiten. La diferencia con las gráficas de tráfico UDP, es que en las de tráfico TCP se distinguen picos verdes ligeramente por debajo de la línea azul, esto es debido a que se genera tráfico en media y cuando se enfrenta tráfico UDP frente a TCP, el UDP no colabora, es decir, no reduce su ventana de transmisión y continúa transmitiendo a la tasa máxima.

En la tabla de resultados 3.22, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.22: Resultados para fuentes UDP y TCP a 2M "Distintos Contratos"

Filter ID	Filter- PKTS	Filter-OCTETS	TRAFFIC PROFILE DISCARD PKTS	BW (Mbps)
UDP 1 (1,4M) 3 (1,8M)	 29254 29254	 31418796 31418796	 0 0	 **2,094586** **2,094586**
TCP 4 (2,6M) 2 (2,2M)	 25882 25866	 31767844 31766724	 0 0	 **2,117856** **2,117781**

Todos los clientes obtienen el mismo ancho de banda.
Al **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **2,1M**.

Nota: el programa generador *Traffic Generator* genera tráfico en media.

3. **Tráfico generado por cada cliente: 3 Mbps**

   Tráfico total generado: 3 * 4 = 12 Mbps, 120% del ancho de banda total. Por tanto, se forma **cuello de botella en** el enlace final.

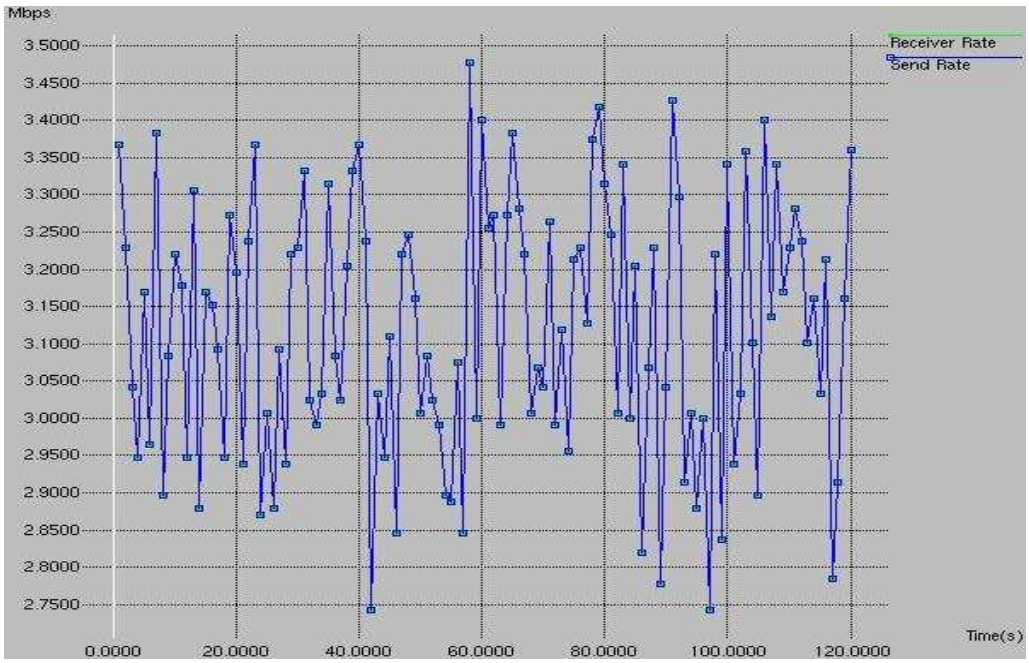


Figura 3.50: C1 (1,4M) UDP PLATA a 3M

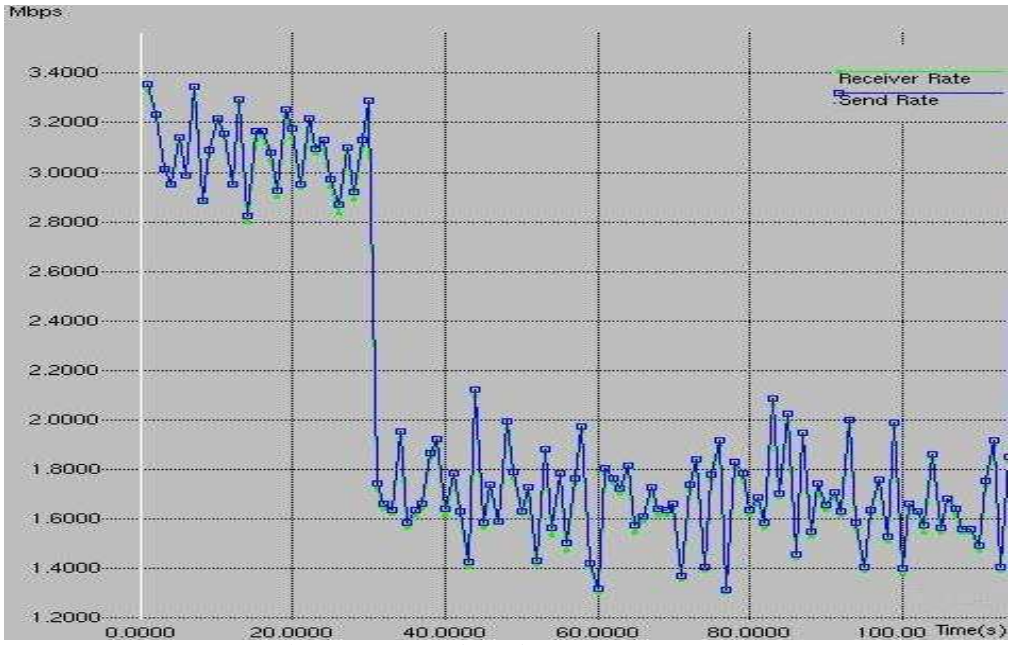


Figura 3.51: C2 (2,2M) TCP PLATA a 3M

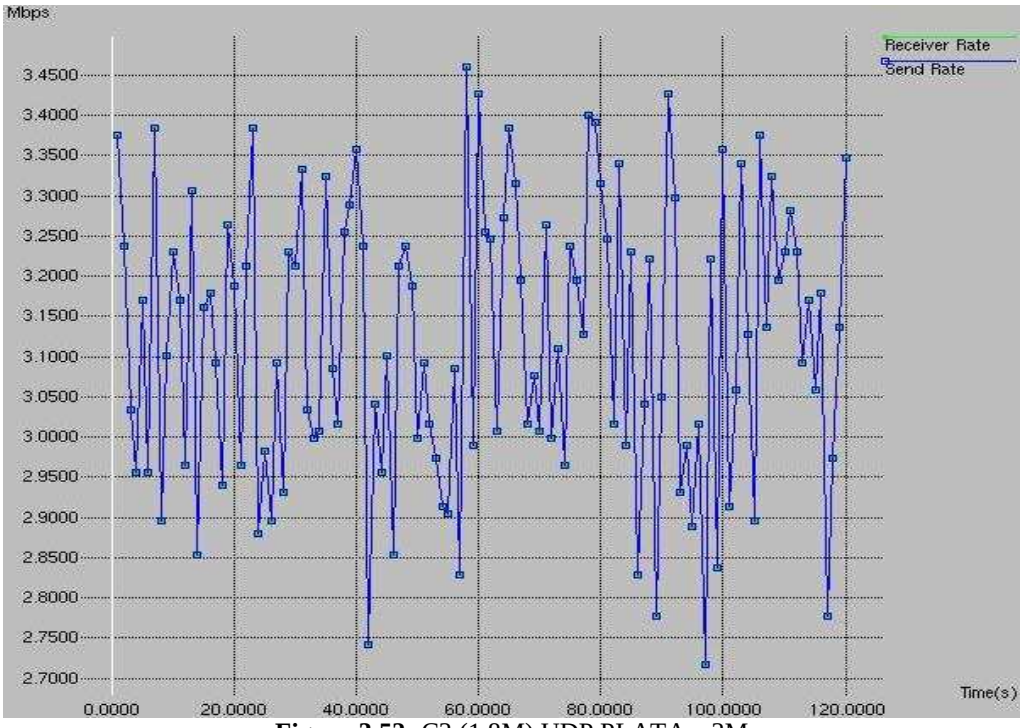


Figura 3.52: C3 (1,8M) UDP PLATA a 3M

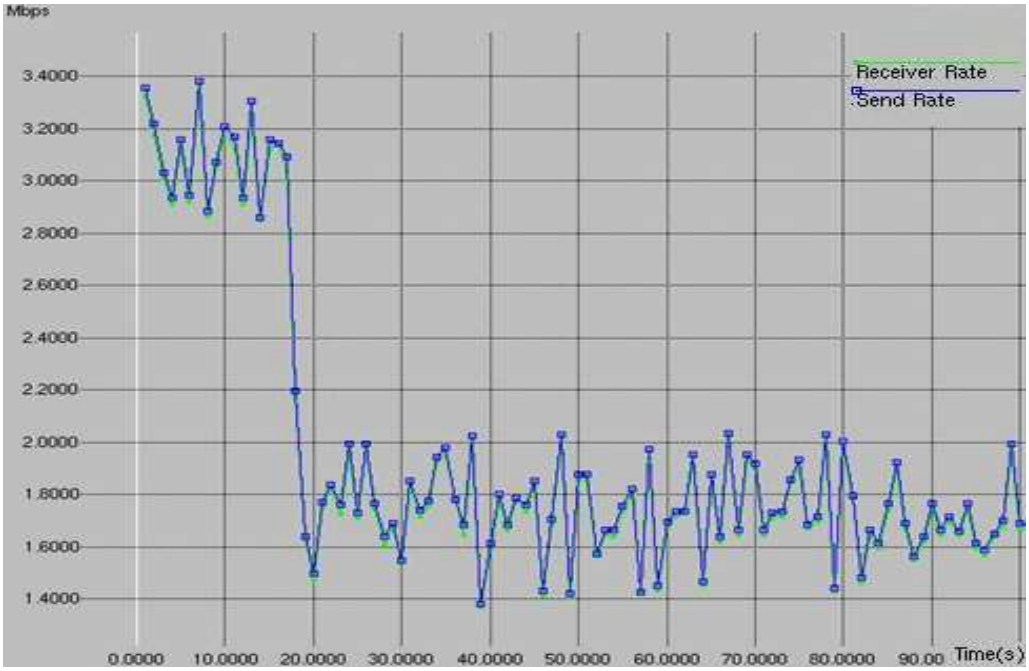


Figura 3.53: C4 (2,6M) TCP PLATA a 3M

En las gráficas de tráfico TCP, clientes C2 y C4, se observa que la línea azul queda ligeramente por encima de la línea verde, ya que en este caso al estar en **situación de congestión** las fuentes TCP no obtienen el ancho de banda máximo al que transmiten.
Se observa como en un principio los **clientes TCP** comienzan a generar tráfico a 3M hasta detectar la congestión. En ese momento, los clientes TCP no obtiene los 3M de ancho de banda a los genera tráfico, ya que al **detectar congestión** reducen su ventana de transmisión.
Los **clientes UDP**, clientes C1 y C3, consiguen los 3M a los que generan tráfico, puesto que las fuentes UDP no se enteran de la congestión y continuarán transmitiendo a la tasa máxima. Del ancho de banda total sobran 2M para cada cliente TCP.

En la tabla de resultados 3.23, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.23: Resultados para fuentes UDP y TCP a 3M "Distintos Contratos"

Filter ID	Filter- PKTS	Filter-OCTETS	TRAFFIC PROFILE DISCARD PKTS	BW (Mbps)
UDP				
1 (1,4M)	43796	47036904	0	**3,13579**
3 (1,8M)	43796	47036904	0	**3,13579**
TCP				
4 (2,6M)	19164	27978900	0	**1,86526**
2 (2,2M)	19142	27947400	0	**1,86316**

Por un lado, los **clientes TCP**, C2 y C4, obtienen un ancho de banda cercano a 2M (**1,86M**), ya que reducen su ventana de transmisión al detectar congestión. Por otro lado, los **clientes UDP**, C1 y C3, obtienen **3,13M** consiguiendo el ancho de banda al que generan tráfico, por tratarse de tráfico UDP.

La suma da 10M que es el total del ancho de banda del enlace. Al estar en situación de congestión, el tráfico UDP va a conseguir el ancho de banda al que genera tráfico, es decir, los clientes C1 y C3 consiguen un total de aproximadamente 6M del ancho de banda total, quedando alrededor de 4M a repartir entre los clientes C2 y C4. Al generar éstos tráfico TCP, y estar en situación de congestión, TCP avisa que se **disminuya la tasa de generación de paquetes**, optando cada cliente a conseguir en torno a 2M del ancho de banda del enlace final.

3.3.3.1.2 Aplicando Servicios Diferenciados (se activa DROP)

a. Mismo contrato

ii. Tráfico generado TCP: todas las fuentes son TCP y tienen el mismo contrato.

1. **Tráfico generado por cada cliente: 1,25 Mbps**

   Tráfico total generado: 1,25 * 4 = 5 Mbps, 50% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

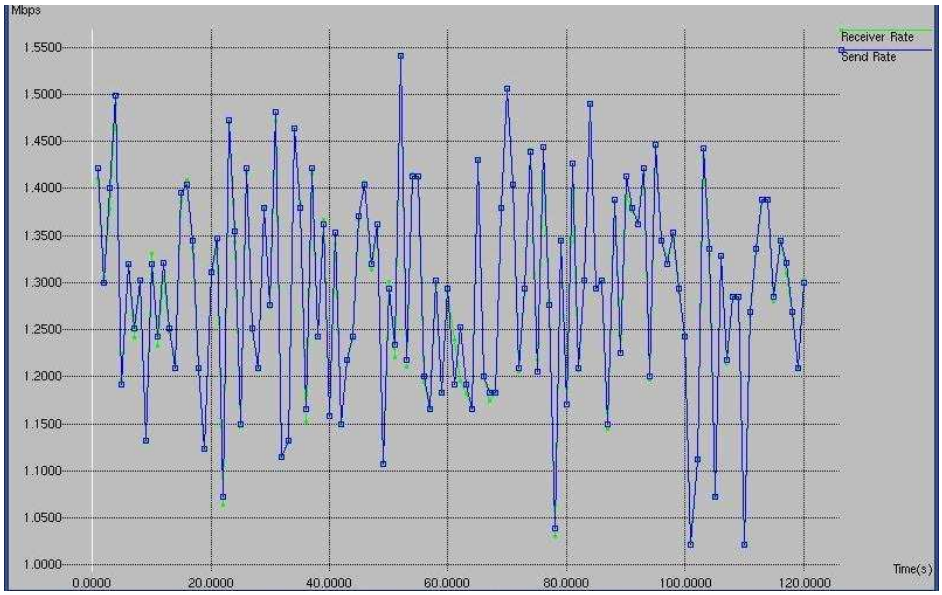


Figura 3.54: C1 (2M) PLATA DROP a 1,25M

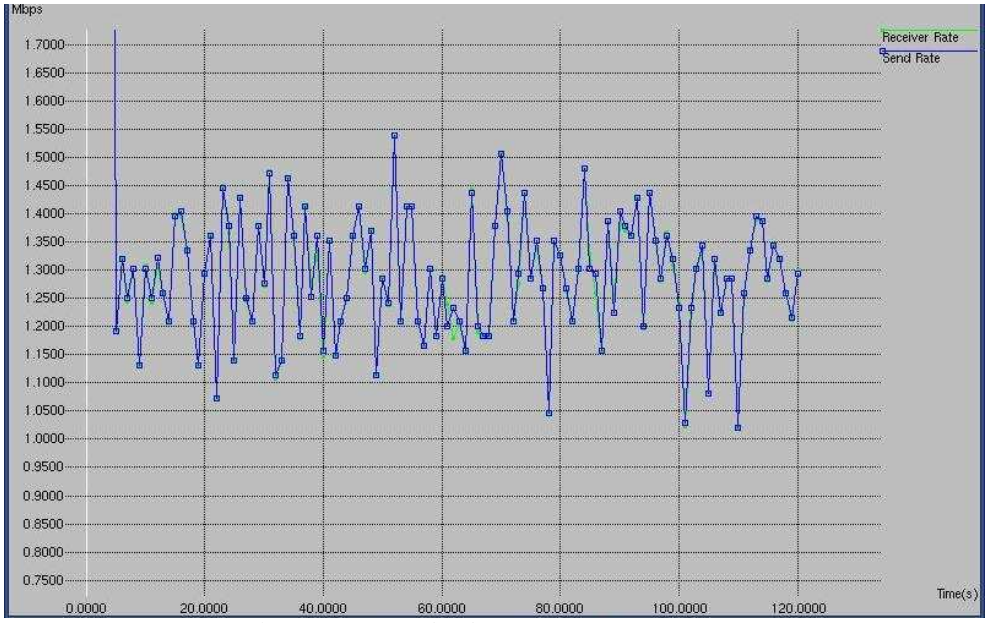


Figura 3.55: C2 (2M) PLATA DROP a 1,25M

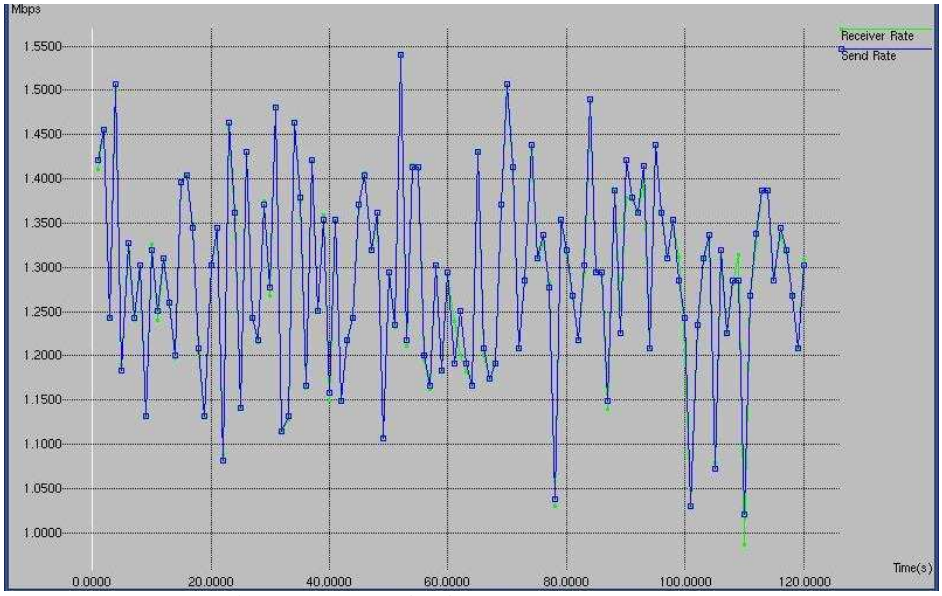


Figura 3.56: C3 (2M) PLATA DROP a 1,25M

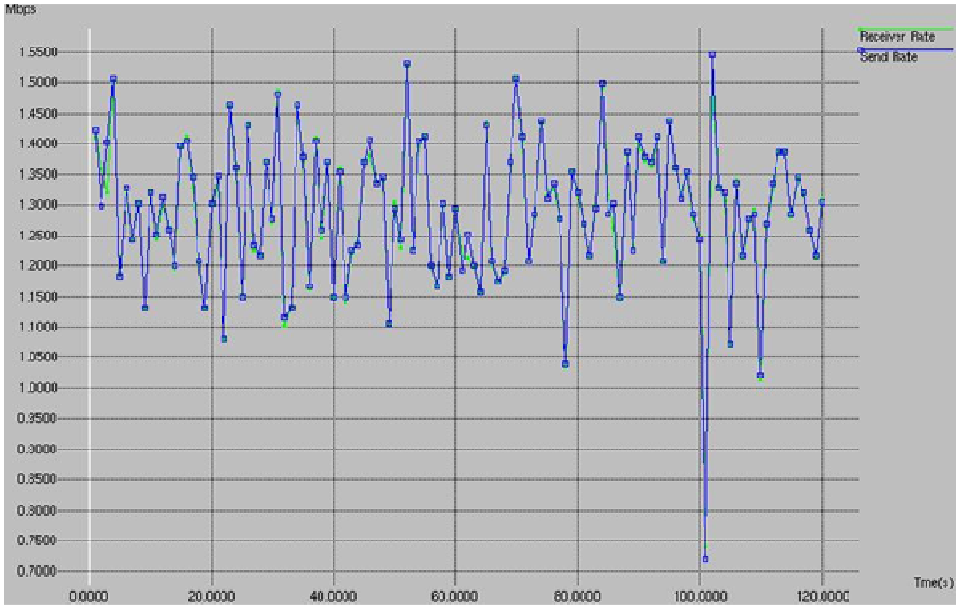


Figura 3.57: C4 (2M) PLATA DROP a 1,25M

En todas las gráficas se observa que la línea azul coincide con la línea verde, con lo cual todos los clientes obtienen el ancho de banda al que transmiten.
Comparando con las gráficas cuando **no se aplican servicios diferenciados**, se aprecian **picos más pronunciados** y **aislados** debido a que ahora se descartan los paquetes que superen el contrato de los clientes (2M).

En la tabla de resultados 3.24, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.24: Resultados para todas las fuentes TCP a 1,25M "Mismo Contrato" 2M DROP

Filter ID	Filter-PKTS	Filter-OCTETS	Ventana de transmisión	TRAFFIC PROFILE DISCARD PKTS	BW DESCARTADO	BW (Mbps)
1	17845	20053678	1,336911	**145**	0,010865	**1,326045**
3	17798	20004484	1,333632	**115**	0,008617	**1,325014**
4	17767	20040690	1,336046	**139**	0,010453	**1,325593**
2	17738	20089108	1,339273	**164**	0,012387	**1,326885**

Todos los clientes obtienen el mismo ancho de banda.
Al tratarse de **sólo tráfico TCP** y **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **1,32M**.

Nota: el programa generador *Traffic Generator* genera tráfico en media.

El **descarte de paquetes** se debe a que el *Traffic Generator* genera en media 1,25Mbps, por lo que se generan paquetes que superan el contrato de 2M. Por tanto **no es significativo**, ya que no existe congestión y las fuentes generan por debajo de su contrato.

2. Tráfico generado por cada cliente: 2 Mbps

Tráfico total generado: 2 * 4 = 8 Mbps, 80% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

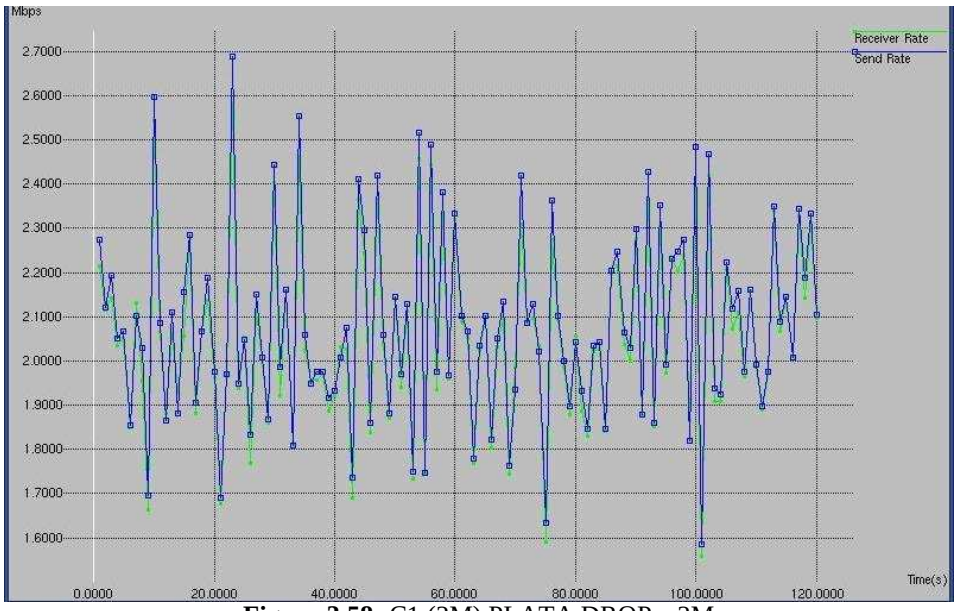


Figura 3.58: C1 (2M) PLATA DROP a 2M

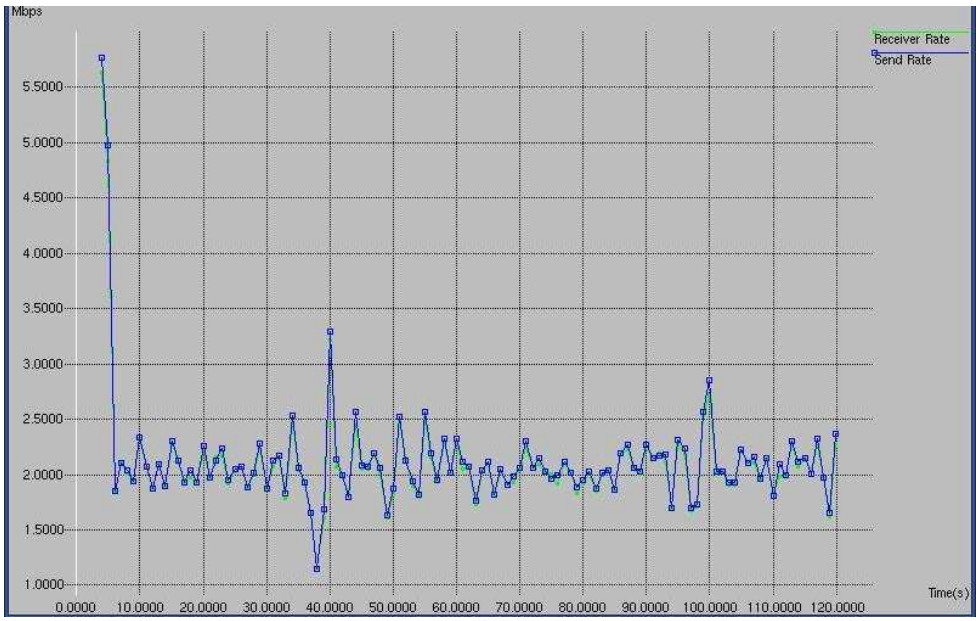


Figura 3.59: C2 (2M) PLATA DROP a 2M

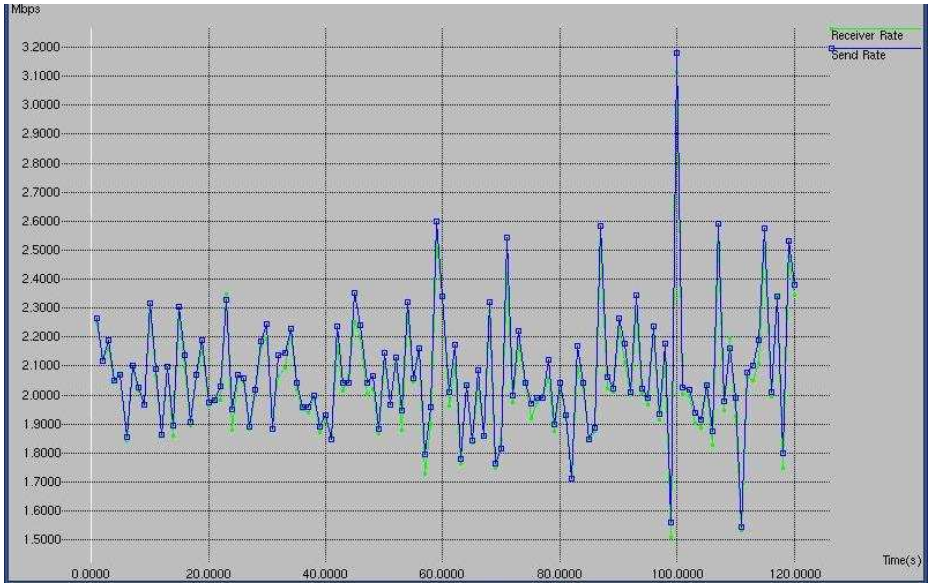


Figura 3.60: C3 (2M) PLATA DROP a 2M

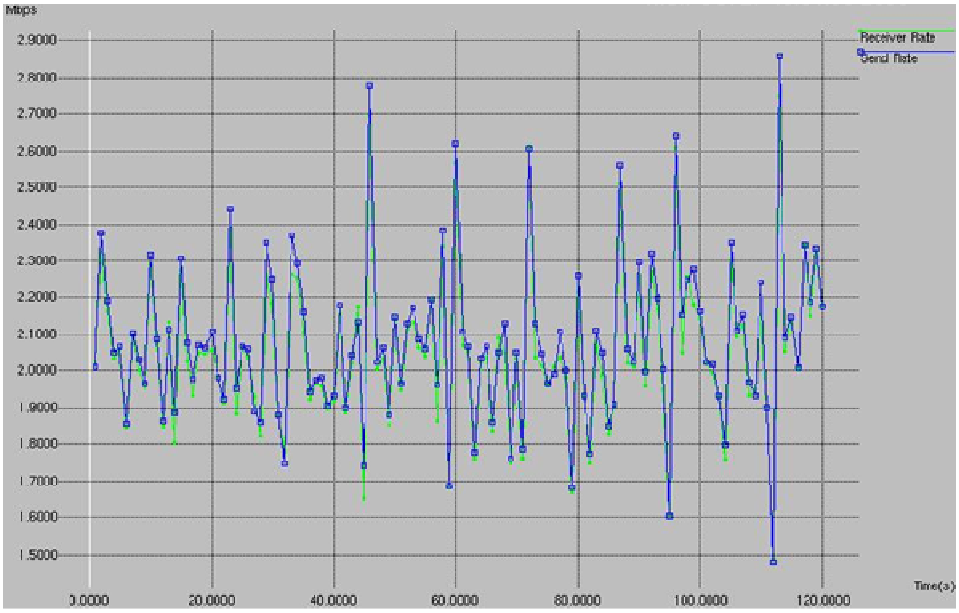


Figura 3.61: C4 (2M) PLATA DROP a 2M

En todas las gráficas se observa que la línea azul prácticamente coincide con la línea verde, con lo cual todos los clientes obtienen el ancho de banda al que transmiten.
Comparando con las gráficas cuando **no se aplican servicios diferenciados**, se aprecian **picos más pronunciados** y **aislados** debido a que ahora se descartan los paquetes que superen el contrato de los clientes (2M).

En la tabla de resultados 3.25, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.25: Resultados para todas las fuentes TCP a 2M "Mismo Contrato" 2M DROP

Filter ID	Filter-PKTS	Filter-OCTETS	Ventana de transmisión	TRAFFIC PROFILE DISCARD PKTS	BW DESCARTADO	BW (Mbps)
1	25887	33108474	2,20723	**1077**	0,091832	**2,115398**
3	25619	33375066	2,225	**1242**	0,107888	**2,117115**
4	25576	33451544	2,2301	**1319**	0,115016	**2,115085**
2	25269	33233262	2,21555	**1235**	0,108268	**2,107281**

Todos los clientes obtienen el mismo ancho de banda.
Al tratarse de **sólo de tráfico TCP** y **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **2,1M**.

El **descarte** de paquetes es **equitativo**, ya que todos los clientes tienen el mismo contrato (2M), y son fuentes TCP. Se observa que pierden entorno a **0,1M** respecto al ancho de banda al que generan tráfico.

Nota: Cuando se aplican Servicios Diferenciados activándose el descarte de paquetes DROP, aunque no se esté en situación de congestión, se produce descarte de paquetes debido a que el programa generador de tráfico *Traffic Generator* genera el tráfico de forma aleatoria, es decir, genera en media, por lo que se generan paquetes que superan el contrato de 2M.

3. Tráfico generado por cada cliente: 3 Mbps

Tráfico total generado: 3 * 4 = 12 Mbps, 120% del ancho de banda total. Por tanto, se forma **cuello de botella en** el enlace final.

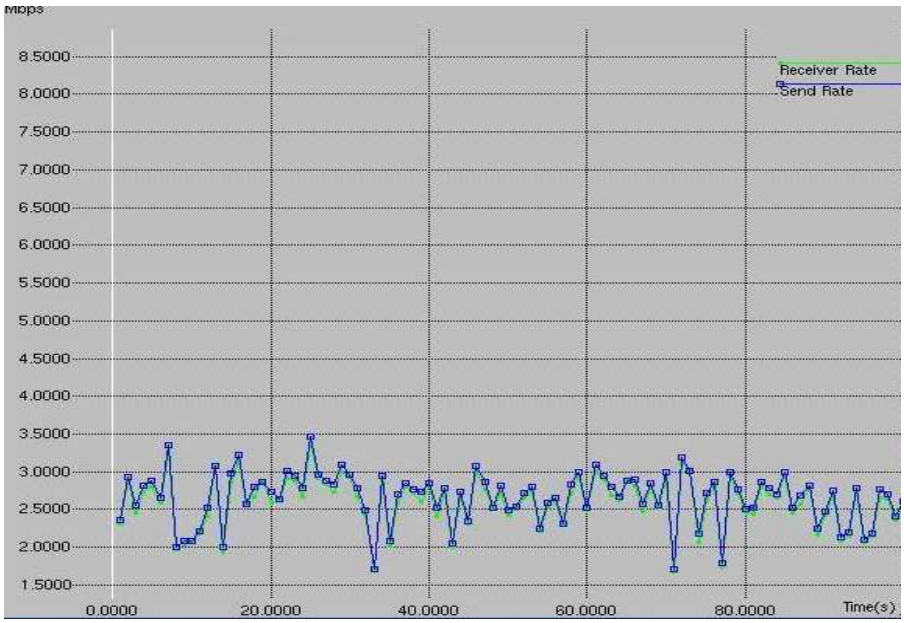


Figura 3.62: C1 (2M) PLATA DROP a 3M

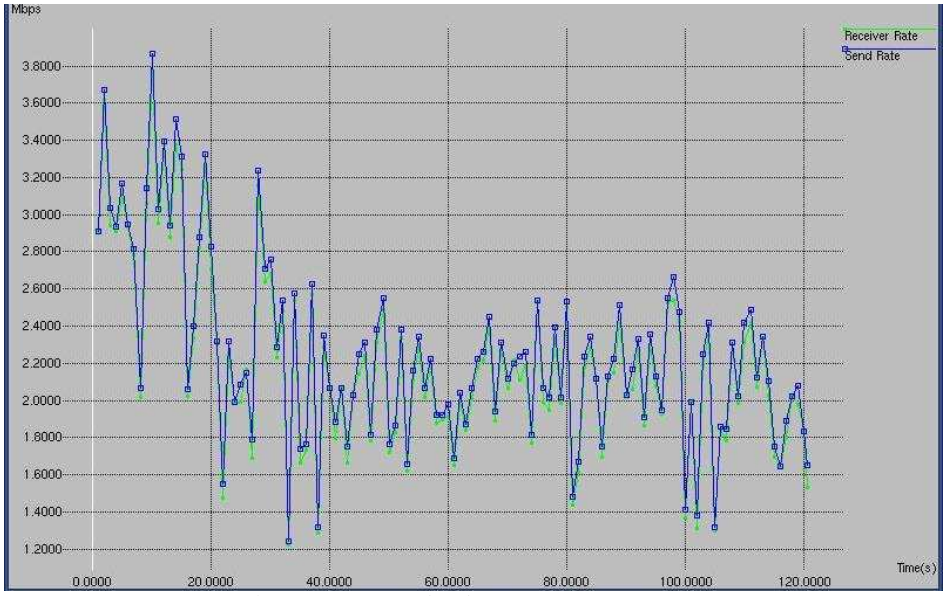


Figura 3.63: C2 (2M) PLATA DROP a 3M

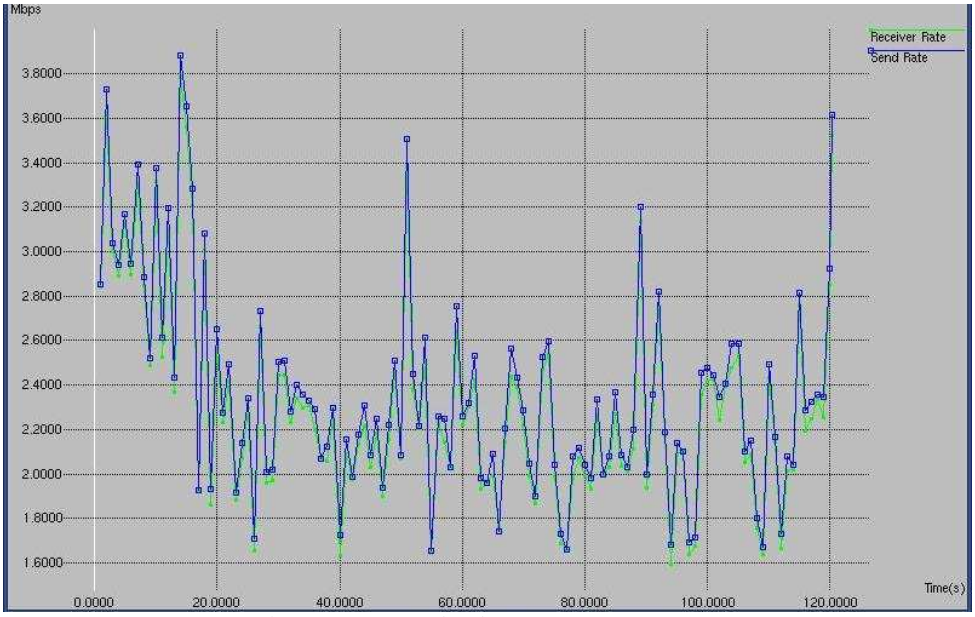


Figura 3.64: C3 (2M) PLATA DROP a 3M

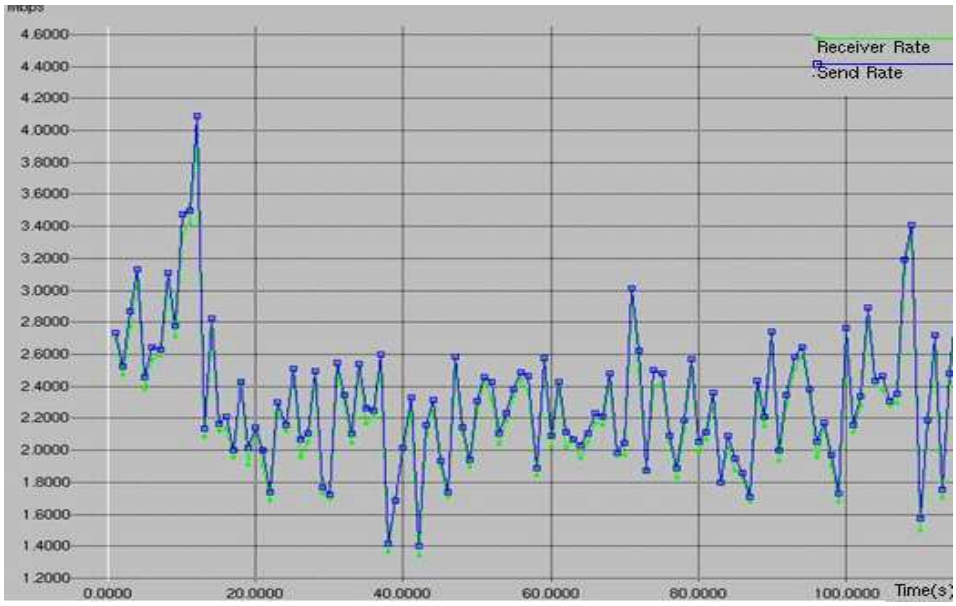


Figura 3.65: C4 (2M) PLATA DROP a 3M

En todas las gráficas se observa que la línea azul queda ligeramente por encima de la línea verde, ya que en este caso al estar en **situación de congestión** y ser todas las fuentes TCP, los clientes no obtienen el ancho de banda al que transmiten.
Cada cliente puede obtener como máximo 10/4 = 2,5M del ancho de banda total. Se reparte los 10M del enlace final entre los cuatro clientes TCP, equitativamente. Se observa como en un principio todos los clientes comienzan a generar a 3M hasta detectar la congestión. Señalar que en la gráfica del cliente C1, al empezar a transmitir más tarde, directamente transmite a la ventana de transmisión (2,5M en media) que le corresponde en esta situación de congestión.
Cada cliente no obtiene los 3M de ancho de banda a los genera tráfico, sino que al **detectar congestión** reducen su ventana de transmisión, llevándose por tanto 2,5M (en media) del canal, esto es, aproximadamente la cuarta parte de los 10M del canal.

La diferencia respecto a las gráficas obtenidas en el caso "Sin aplicar Servicios Diferenciados" se aprecia en que aparecen picos más pronunciados y aislados, debido a que ahora se descartan los paquetes que superen el contrato de los clientes (2M). Se observa, cómo cuando las fuentes TCP comienzan a transmitir a 3M, ahora la transmisión, es menos uniforme, es decir, presenta picos más pronunciados y espaciados. Así se aprecia el fenómeno de descarte.

En la tabla de resultados 3.26, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.26: Resultados para todas las fuentes TCP a 3M "Mismo Contrato" 2M DROP

Filter ID	Filter-PKTS	Filter-OCTETS	Ventana de transmisión	TRAFFIC PROFILE DISCARD PKTS	BW DESCARTADO	BW (Mbps)
1	27460	41190225	2,746015	**2072**	0,2071	**2,538855**
3	26381	39471190	2,631412	**1585**	0,1581	**2,473302**
4	26693	40361398	2,690759	**1728**	0,1742	**2,516482**
2	26286	39140190	2,609346	**1329**	0,1319	**2,477359**

Se observa cómo prácticamente se obtiene el mismo ancho de banda para todos, en torno a 2,5M. El descarte de paquetes es mayor para las fuentes que transmiten a mayor velocidad para equipararlas con las que transmiten a menor velocidad. Cada fuente recibe aproximadamente **0,5M** del ancho de banda no contratado. Por tanto, vemos como que para fuentes TCP con el mismo contrato de 2M **el reparto es equitativo**.

ii. Tráfico generado UDP y TCP

En esta prueba, los **contratos** de las fuentes generadoras de tráfico **TCP** C2 y C4 son **mayores** que los contratos de las fuentes generadoras de tráfico **UDP** C1 y C3.

1. Tráfico generado por cada cliente: 1,25 Mbps

Tráfico total generado: 1,25 * 4 = 5 Mbps, 50% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

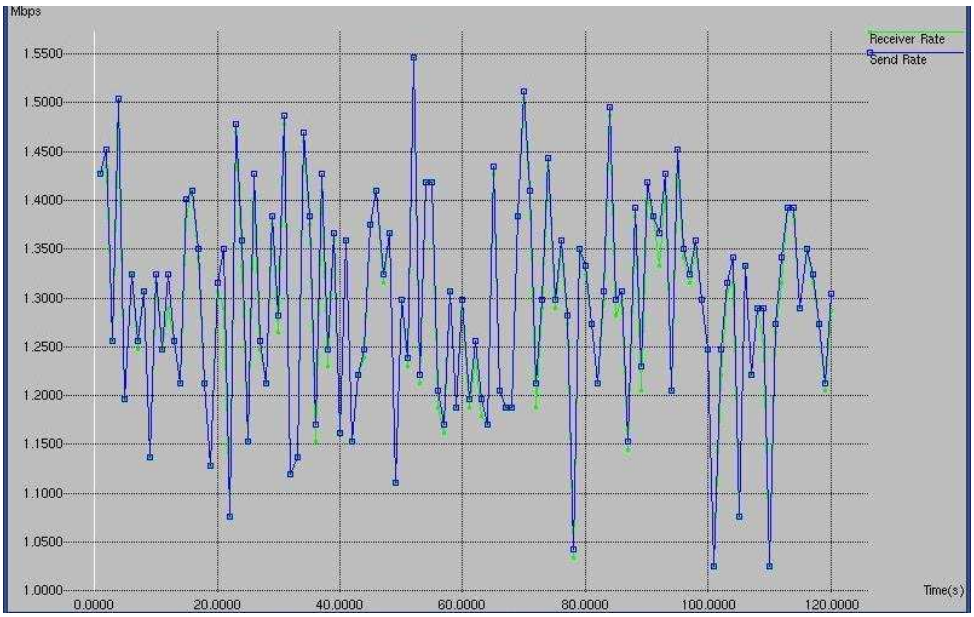


Figura 3.66: C1 (2M) UDP PLATA a 1,25M

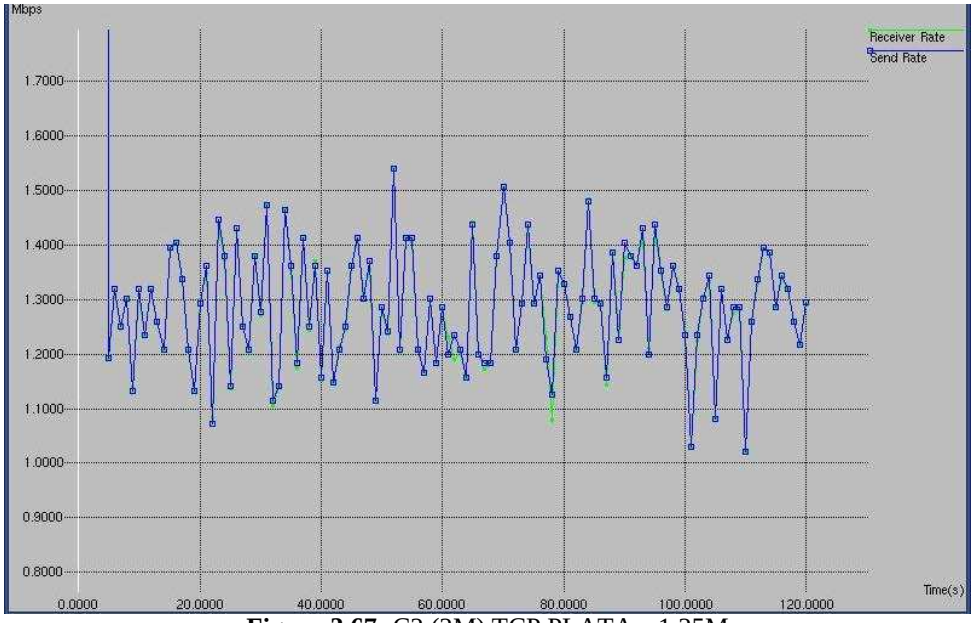


Figura 3.67: C2 (2M) TCP PLATA a 1,25M

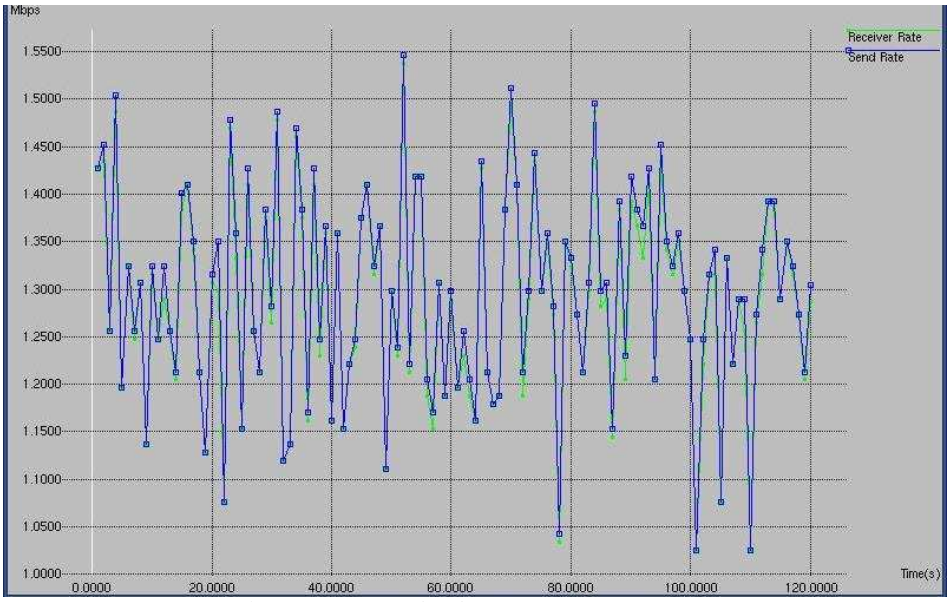


Figura 3.68: C3 (2M) UDP PLATA a 1,25M

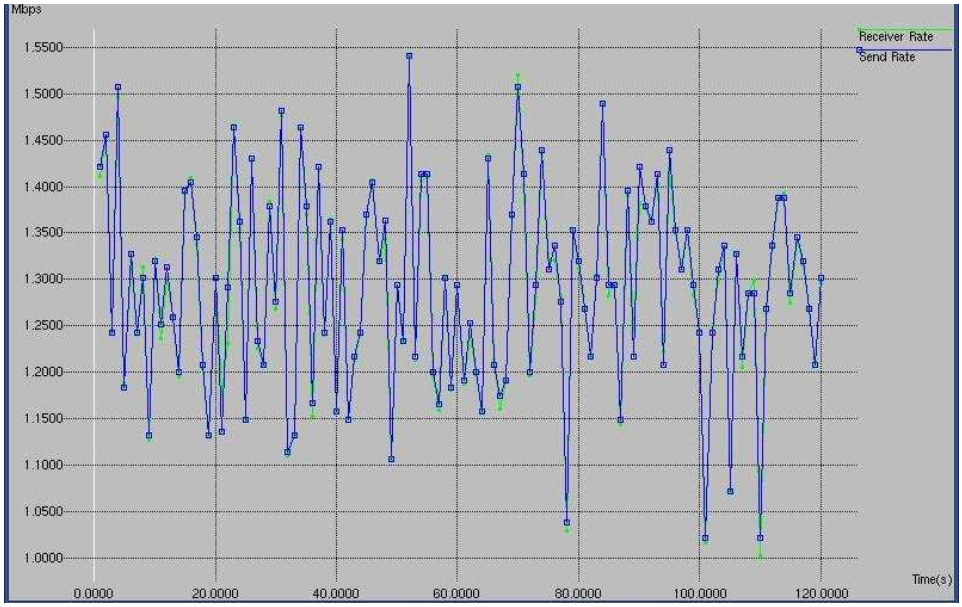


Figura 3.69: C4 (2M) TCP PLATA a 1,25M

En todas las gráficas se observa que prácticamente la línea azul coincide con la línea verde, con lo cual todos los clientes obtienen el ancho de banda al que transmiten. La diferencia con el caso en el que no hay descarte, es que ahora, se aprecian **tramos verdes, también en las fuentes UDP,** que no coinciden exactamente con la línea azul quedando ligeramente por debajo debido a los descartes. Estos descartes son debidos a que se genera en media, por tanto **no son significativos**, ya que no se está en situación de congestión, es decir, hay ancho de banda de sobra.

En la tabla de resultados 3.27, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.27: Resultados para fuentes UDP y TCP a 1,25M "Mismo Contrato" 2M DROP

Filter ID	Filter-PKTS	Filter-OCTETS	Ventana de transmisión	TRAFFIC PROFILE DISCARD PKTS	BW DESCARTADO	BW (Mbps)
UDP						
1	18194	19540356	1,30269	**112**	0,008019	**1,294671**
3	18194	19540356	1,30269	**112**	0,008019	**1,294671**
TCP						
4	17686	20010372	1,334024	**127**	0,009584	**1,324439**
2	17645	20071078	1,338071	**156**	0,011835	**1,326235**

Todos los clientes obtienen prácticamente el mismo ancho de banda. Al **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **1,3M**.

Los descartes de paquetes no son significativos, ya que es por generar tráfico en media, y no porque falte ancho de banda.

Nota: el programa generador *Traffic Generator* genera tráfico en media.

2. Tráfico generado por cada cliente: 2 Mbps

Tráfico total generado: 2 * 4 = 8 Mbps, 80% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

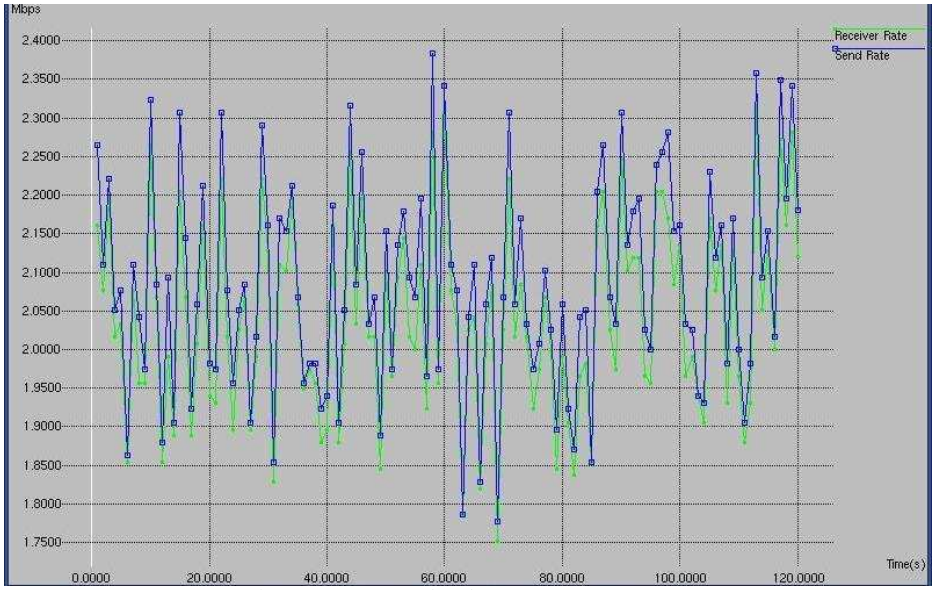


Figura 3.70: C1 (2M) UDP PLATA a 2M

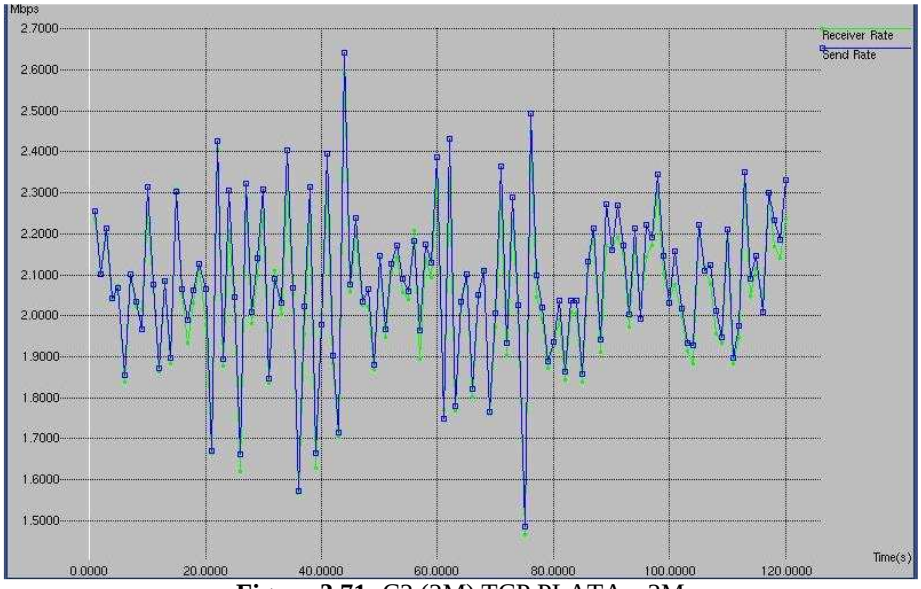


Figura 3.71: C2 (2M) TCP PLATA a 2M

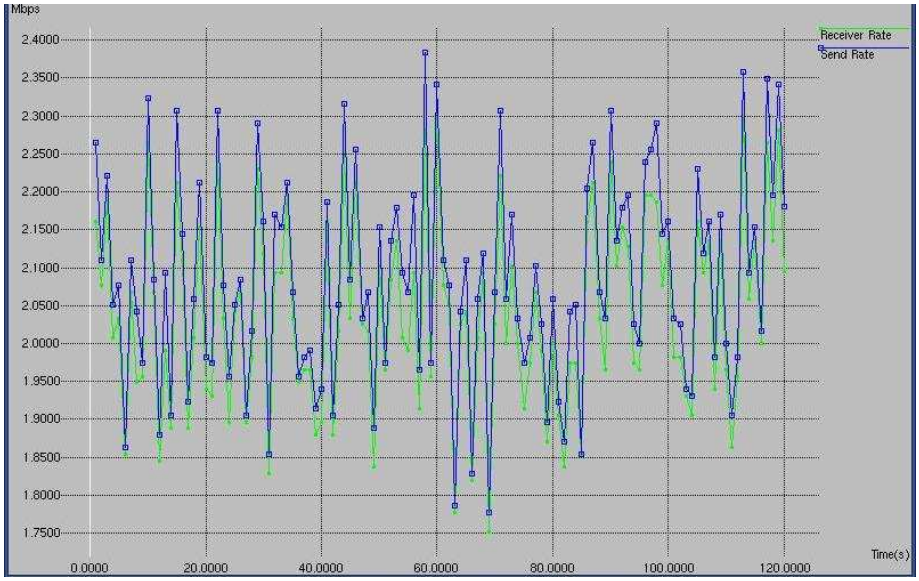


Figura 3.72: C3 (2M) UDP PLATA a 2M

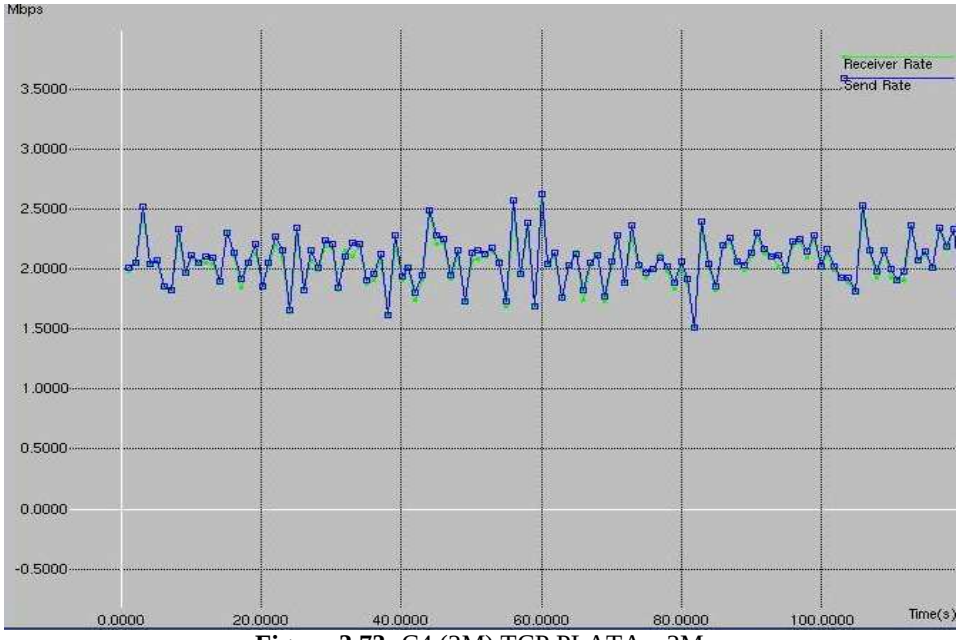


Figura 3.73: C4 (2M) TCP PLATA a 2M

En este escenario se ocupa el 80% del canal, con lo cual se está en el límite a partir del cual las prestaciones de la red comienzan a degradarse. Pasado este límite el tráfico UDP acapara los recursos frente al tráfico TCP.

Al aplicar Servicios Diferenciados, se observa que en las gráficas de tráfico UDP, clientes C1 y C3, la línea azul y la verde se separan ligeramente. Esto es debido a los descartes que sufre. Aún así, obtiene el ancho de banda al que transmite, ya que **hay ancho de banda de sobra** para todas las fuentes.

Por otro lado, en las gráficas de tráfico TCP, clientes C2 y C4 se aprecia que la línea azul prácticamente coincide con la línea verde, con lo cual los clientes TCP obtienen el ancho de banda al que transmiten.

En la tabla de resultados 3.28, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.28: Resultados para fuentes UDP y TCP a 2M "Mismo Contrato" 2M DROP

Filter ID	Filter-PKTS	Filter-OCTETS	Ventana de transmisión	TRAFFIC PROFILE DISCARD PKTS	BW DESCARTADO	BW (Mbps)
UDP						
1	29254	31418796	2,094586	**619**	0,044321	**2,052329**
3	29252	31416648	2,094443	**618**	0,044248	**2,050195**
TCP						
4	25514	33625068	2,241671	**1497**	0,131536	**2,110134**
2	25681	33460894	2,230726	**1327**	0,115272	**2,115454**

Todos los clientes obtienen el mismo ancho de banda.
Al **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **2,08M**.

Nota: el programa generador *Traffic Generator* genera tráfico en media.

El tráfico TCP sufre más descartes que el UDP, **debido al propio descarte**, ya que TCP detecta las pérdidas y **reenvía los paquetes descartados**.

3. Tráfico generado por cada cliente: 3 Mbps

Tráfico total generado: 3 * 4 = 12 Mbps, 120% del ancho de banda total. Por tanto, se forma **cuello de botella en** el **enlace final.**

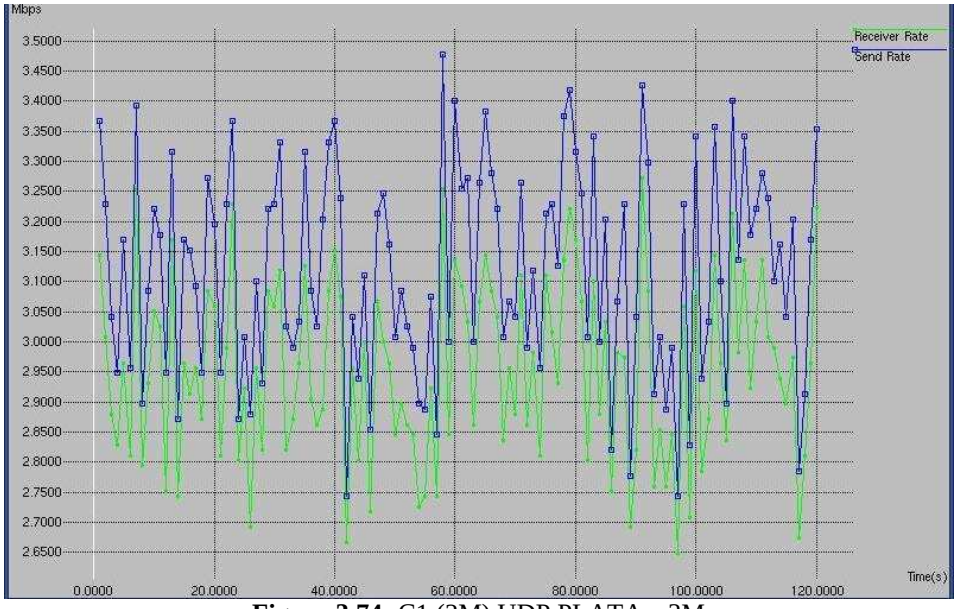


Figura 3.74: C1 (2M) UDP PLATA a 3M

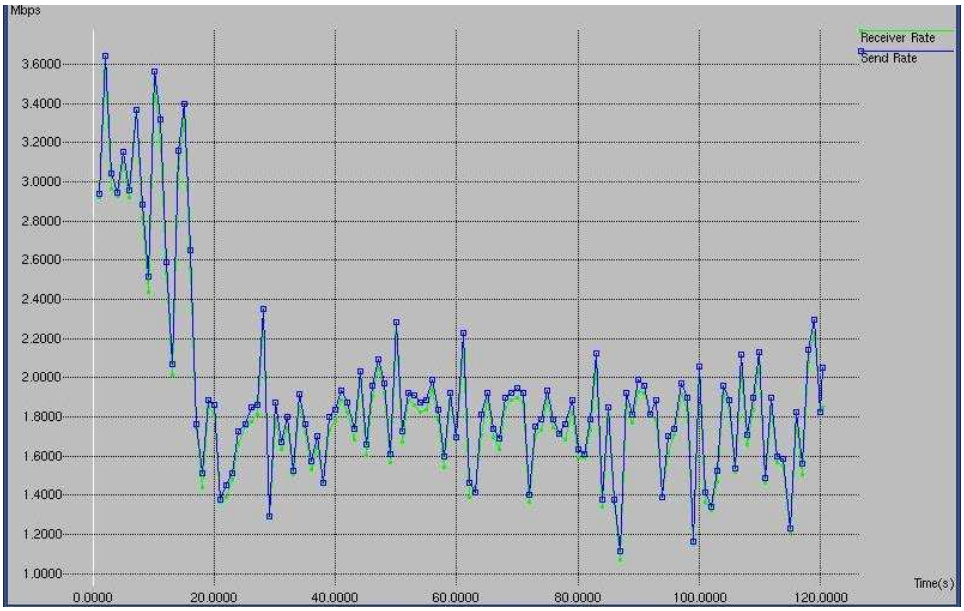


Figura 3.75: C2 (2M) TCP PLATA a 3M

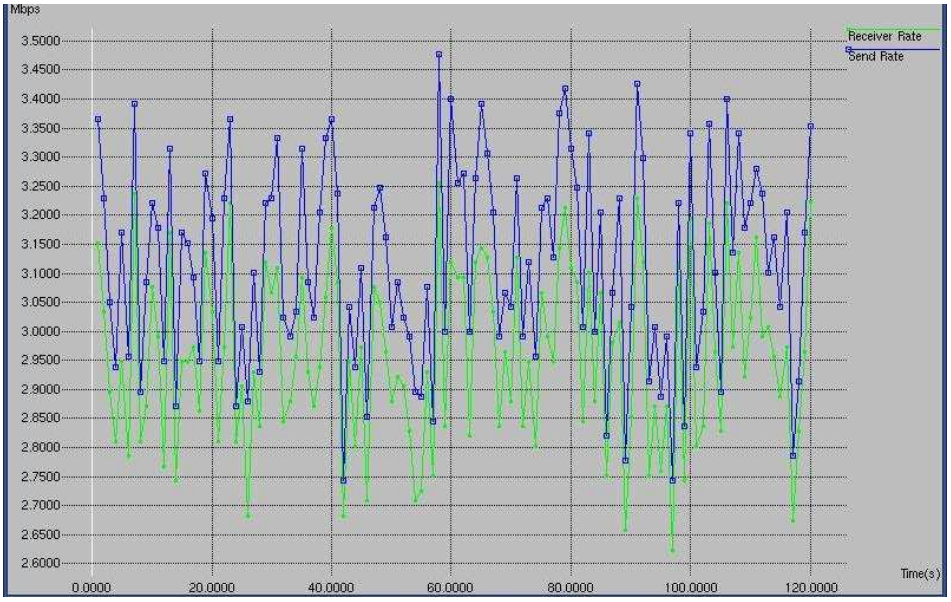


Figura 3.76: C3 (2M) UDP PLATA a 3M

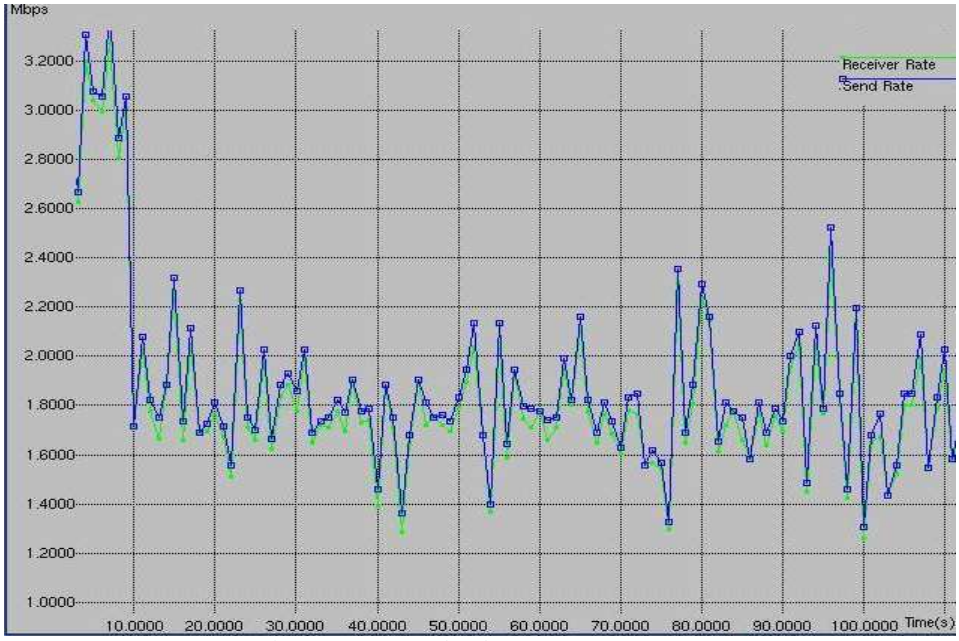


Figura 3.77: C4 (2M) TCP PLATA a 3M

En las gráficas de tráfico TCP, clientes C2 y C4, se observa como en un principio los **clientes TCP** comienzan a generar tráfico a 3M hasta detectar la congestión. En ese momento, los clientes TCP no transmiten a los 3M de ancho de banda a los genera tráfico, sino que reducen su ventana de transmisión. Se aprecia que la línea azul queda ligeramente por encima de la línea verde, **debido al descarte de paquetes**, por estar activada la diferenciación de servicios.
En las gráficas de tráfico UDP, clientes C1 y C3, se observa una evidente separación entre la línea azul y la línea verde, que es mayor que en las fuentes de tráfico TCP, debida a que estas fuentes **generan tráfico a 3M durante toda la transmisión** y al ser el contrato de 2M el descarte de paquetes es mayor.
Los **clientes UDP**, clientes C1 y C3, consiguen los 3M a los que generan tráfico, puesto que las fuentes UDP no se enteran de la congestión. Sobran 2M para cada cliente TCP.

En la tabla de resultados 3.29, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.29: Resultados para fuentes UDP y TCP a 3M "Mismo Contrato" 2M DROP

Filter ID	Filter-PKTS	Filter-OCTETS	Ventana de transmisión	TRAFFIC PROFILE DISCARD PKTS	BW DESCARTADO	BW (Mbps)
UDP						
1	43794	47034756	3,13565	**2308**	0,157559	**2,97809**
3	43796	47036904	3,13579	**2257**	0,154077	**2,981715**
TCP						
4	23251	35108818	2,340587	**2308**	0,157559	**2,183028**
2	21741	32384766	2,158984	**2077**	0,141789	**2,017194**

Al estar en situación de congestión y tener todas las fuentes el mismo contrato 2M, los descartes en las fuentes UDP aumentan equiparándose a los **descartes** de las fuentes TCP, en torno a **0,15M**. La diferencia radica en que el descarte en las fuentes UDP se debe a que éstas generan tráfico a su máximo 3M **durante toda la transmisión**. Sin embargo, en las fuentes TCP el descarte se debe principalmente al reenvío de los paquetes descartados. Las fuentes TCP disminuyen su ventana de transmisión al detectar congestión. Al aplicar Servicios Diferenciados, los **clientes UDP**, C1 y C3, ya no obtienen el ancho de banda al que generan tráfico 3,13M, sino un poco menos 2,9M. Aún así, este valor está muy próximo a los 3M a los que dichas fuentes generan tráfico, consiguiendo un total de 6M aproximadamente del ancho de banda total, quedando 4M aproximadamente a repartir entre los clientes C2 y C4. Al generar éstos tráfico TCP, y estar en situación de congestión, éste avisa que se **disminuya la tasa de generación de paquetes**, optando cada cliente a conseguir entorno a 2M de ancho de banda del enlace.

b. Distintos contratos

i. Tráfico generado TCP: todas las fuentes son TCP. Los contratos de las fuentes TCP C2 y C4 son **mayores** que los contratos de las fuentes TCP C1 y C3.

1. Tráfico generado por cada cliente: 1,25 Mbps

Tráfico total generado: 1,25 * 4 = 5 Mbps, 50% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

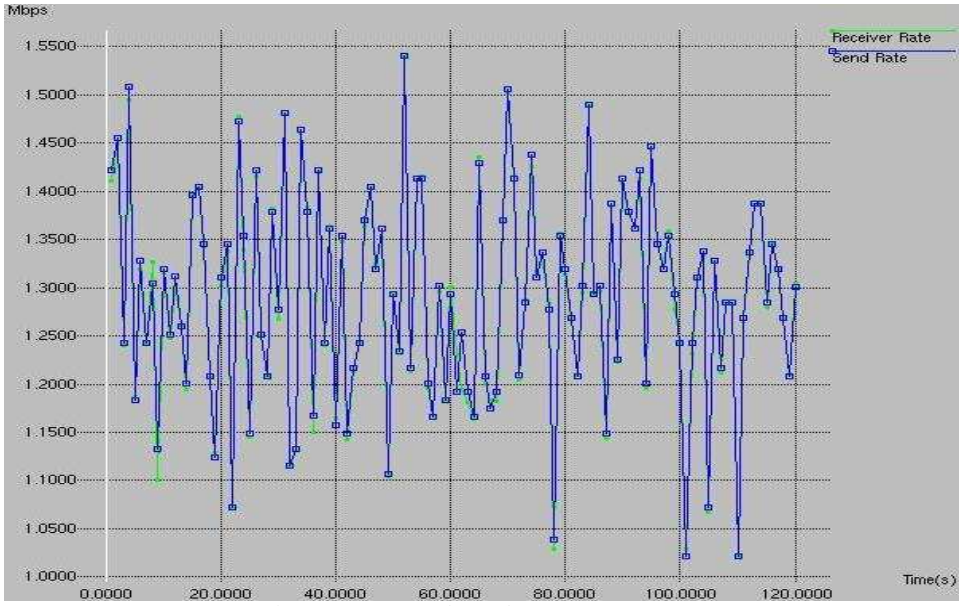


Figura 3.78: C1 (1,4M) PLATA a 1,25M

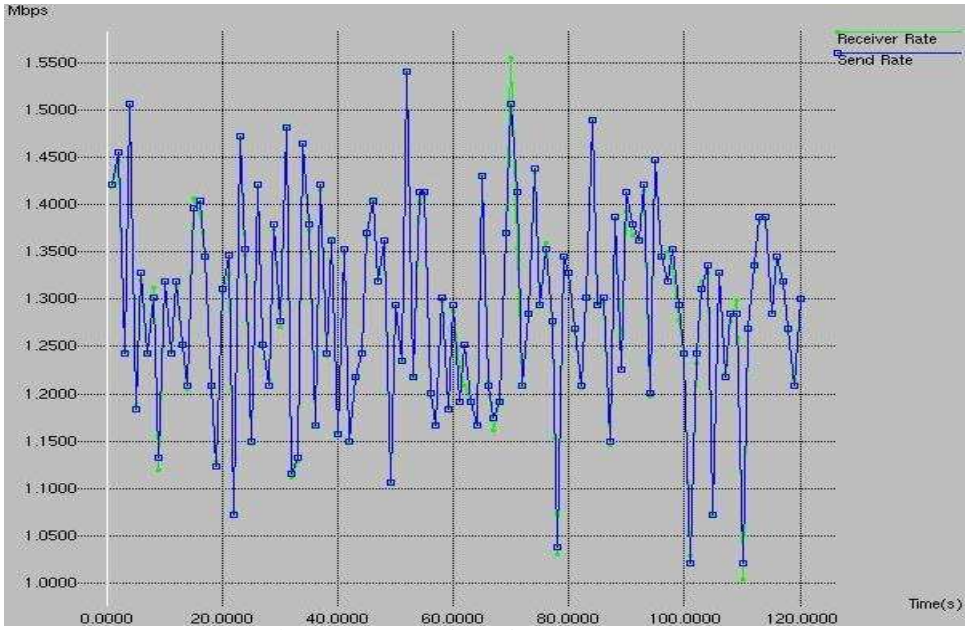


Figura 3.79: C2 (2,2M) PLATA a 1,25M

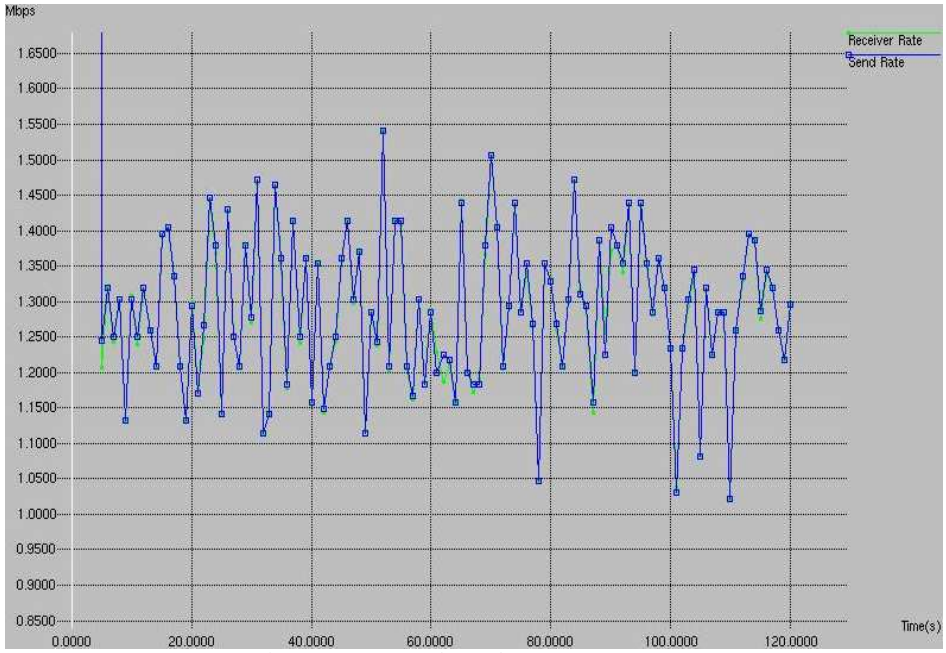


Figura 3.80: C3 (1,8M) PLATA a 1,25M

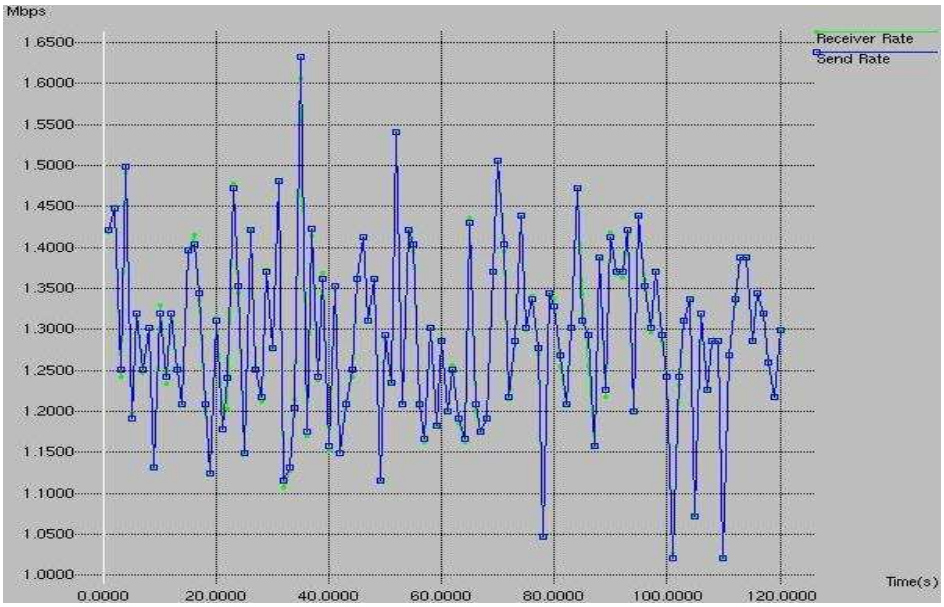


Figura 3.81: C4 (2,6M) PLATA a 1,25M

En todas las gráficas se observa que la línea azul coincide con la línea verde, con lo cual todos los clientes obtienen el ancho de banda al que transmiten.
Comparando con las gráficas cuando **no se aplican servicios diferenciados**, se aprecian **picos más pronunciados** y **aislados** debido a que ahora se descartan los paquetes que superen el contrato de los clientes. Esto se aprecia más en las gráficas de los clientes C1 y C3 donde el contrato es menor.

En la tabla de resultados 3.30, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.30: Resultados para todas las fuentes TCP a 1,25M "Distintos Contratos" DROP

Filter ID	Filter-PKTS	Filter-OCTETS	Ventana de transmisión	TRAFFIC PROFILE DISCARD PKTS	BW DESCARTADO	BW (Mbps)
1 (1,4M)	17787	20040330	1,336022	**136**	0,009284	**1,326737**
3 (1,8M)	17648	20078040	1,338536	**165**	0,011264	**1,327272**
4 (2,6M)	17683	19903582	1,326905	**32**	0,002184	**1,324720**
2 (2,2M)	17744	19934832	1,328988	**61**	0,004164	**1,324824**

Todos los clientes obtienen el mismo ancho de banda.
Al tratarse de **sólo tráfico TCP** y **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **1,32M**.

Nota: el programa generador *Traffic Generator* genera tráfico en media.

El **descarte de paquetes** se debe a que el *Traffic Generator* genera en media 1,25Mbps, por lo que se generan paquetes que superan los contratos de los clientes. Por tanto **no es significativo**, ya que no existe congestión y las fuentes generan por debajo de su contrato. Se aprecia que el descarte de paquetes es mayor en los clientes C1 y C3 pues su contrato es menor que el de las fuentes C2 y C4.

2. Tráfico generado por cada cliente: 2 Mbps

Tráfico total generado: 2 * 4 = 8 Mbps, 80% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

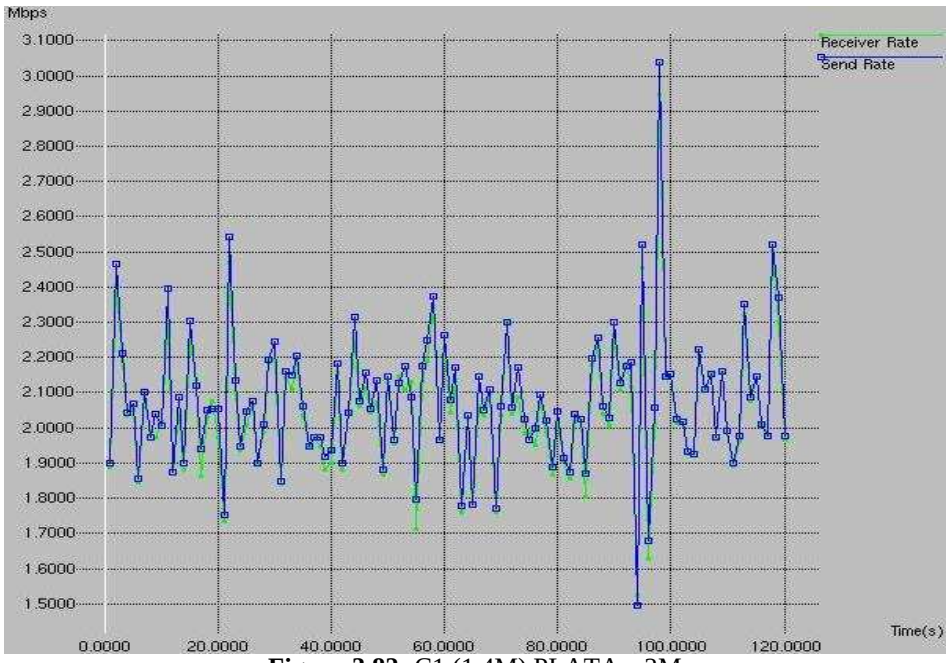


Figura 3.82: C1 (1,4M) PLATA a 2M

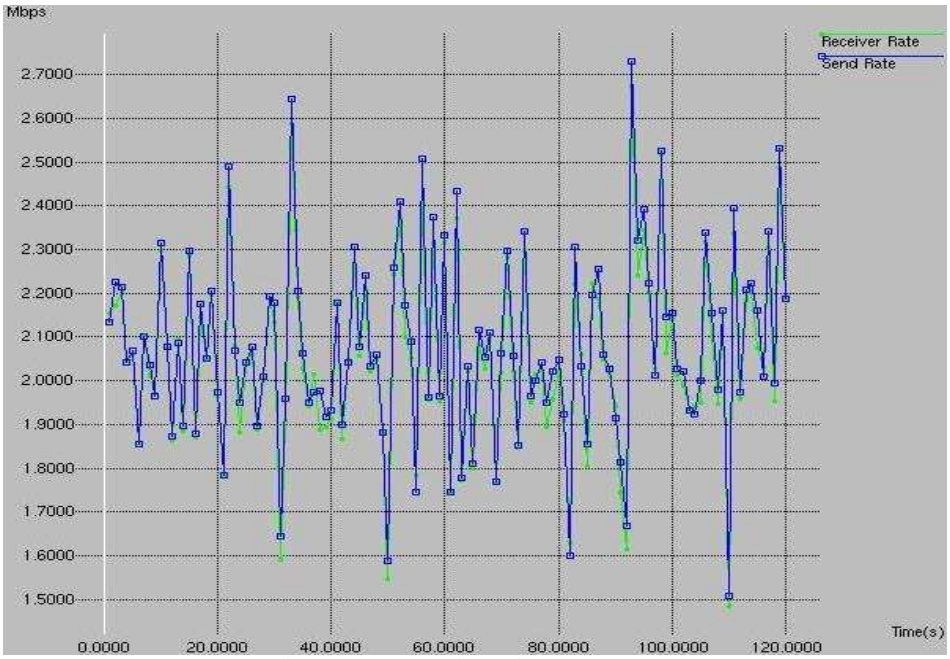


Figura 3.83: C2 (2,2M) PLATA a 2M

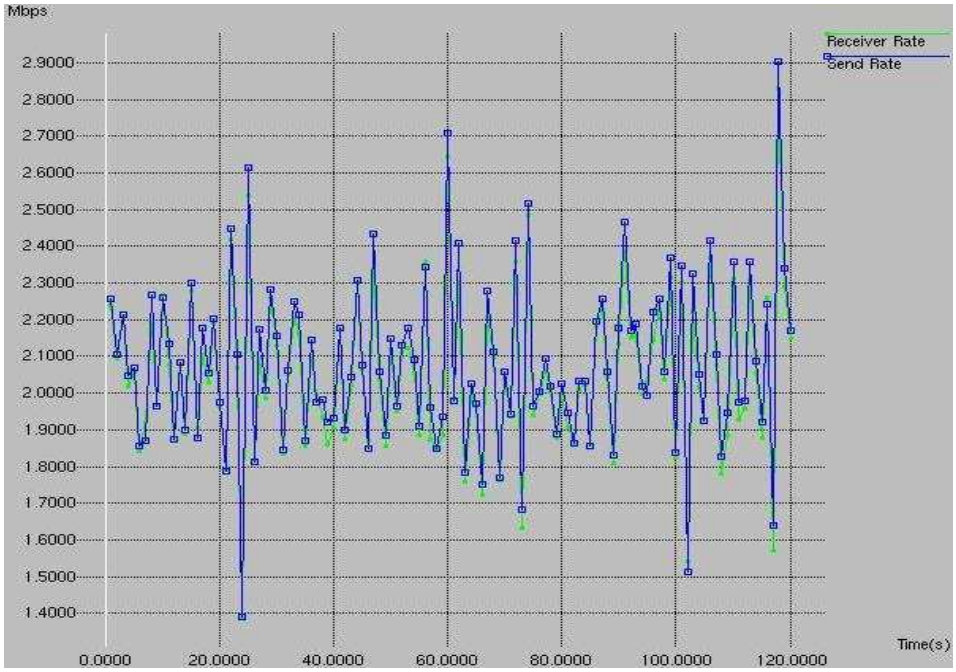


Figura 3.84: C3 (1,8M) PLATA a 2M

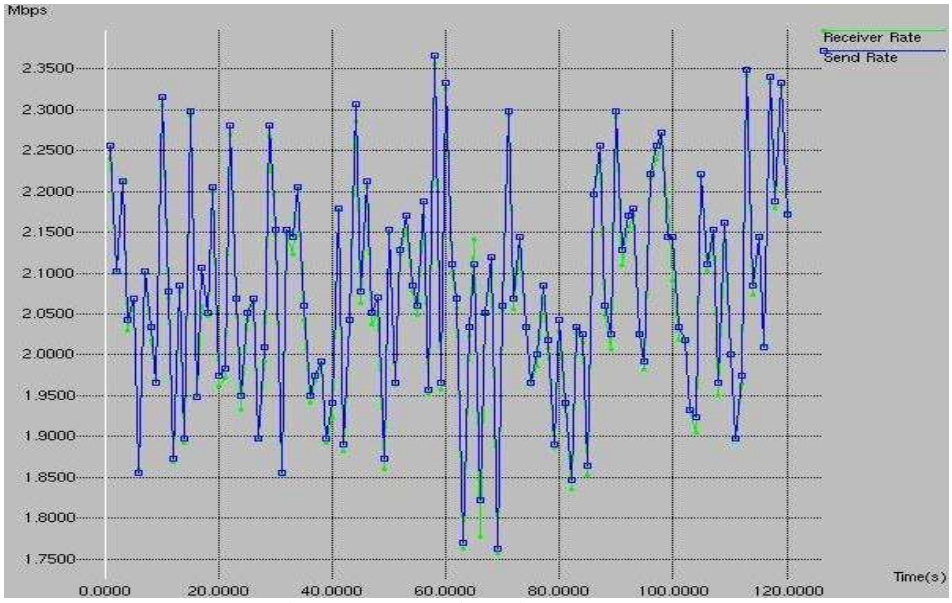


Figura 3.85: C4 (2,6M) PLATA a 2M

En todas las gráficas se observa que la línea azul prácticamente coincide con la línea verde, con lo cual todos los clientes obtienen el ancho de banda al que transmiten.
Comparando con las gráficas cuando **no se aplican servicios diferenciados**, se aprecian **picos más pronunciados** y **aislados** debido a que ahora se descartan los paquetes que superen el contrato de los clientes. Esto se aprecia más en las gráficas de los clientes C1 y C3 donde el contrato es menor.

En la tabla de resultados 3.31, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.31: Resultados para todas las fuentes TCP a 2M "Distintos Contratos" DROP

Filter ID	Filter-PKTS	Filter-OCTETS	Ventana de transmisión	TRAFFIC PROFILE DISCARD PKTS	BW DESCARTADO	BW (Mbps)
1 (1,4M)	25990	33162420	2,210828	**1106**	0,075502	**2,135325**
3 (1,8M)	25580	33433752	2,228916	**1303**	0,088951	**2,139965**
4 (2,6M)	26459	31926178	2,128411	**98**	0,006690	**2,121721**
2 (2,2M)	25626	33053772	2,203584	**1029**	0,070246	**2,133338**

Todos los clientes obtienen el mismo ancho de banda.
Al tratarse de **sólo de tráfico TCP** y **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **2,13M**.

El **descarte** de paquetes depende del contrato de cada cliente y de su ventana de transmisión. Se observa que los clientes C1, C2 y C3, cuyo contrato está por debajo del ancho de banda al que transmiten tráfico TCP (aproximadamente 2,2M), pierden en torno a **0,07M** respecto al ancho de banda al que generan tráfico. El cliente C4 al cumplir el contrato, no sufre pérdidas de paquetes significativas por lo que obtiene justo el ancho de banda al que transmite tráfico.

Nota: Cuando se aplican Servicios Diferenciados activándose el descarte de paquetes DROP, aunque no se esté en situación de congestión, se produce descarte de paquetes debido a que el programa generador de tráfico *Traffic Generator* genera el tráfico de forma aleatoria, es decir, genera en media, por lo que se generan paquetes que superan los contratos de los clientes.

3. Tráfico generado por cada cliente: 3 Mbps

Tráfico total generado: 3 * 4 = 12 Mbps, 120% del ancho de banda total. Por tanto, se forma **cuello de botella en** el **enlace final.**

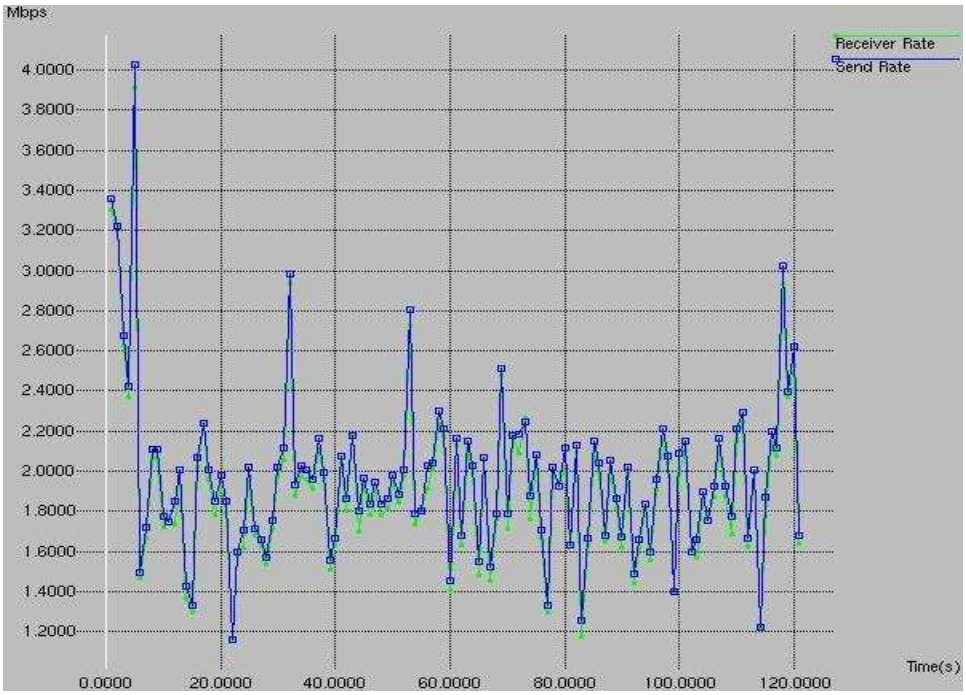


Figura 3.86: C1 (1,4M) PLATA a 3M

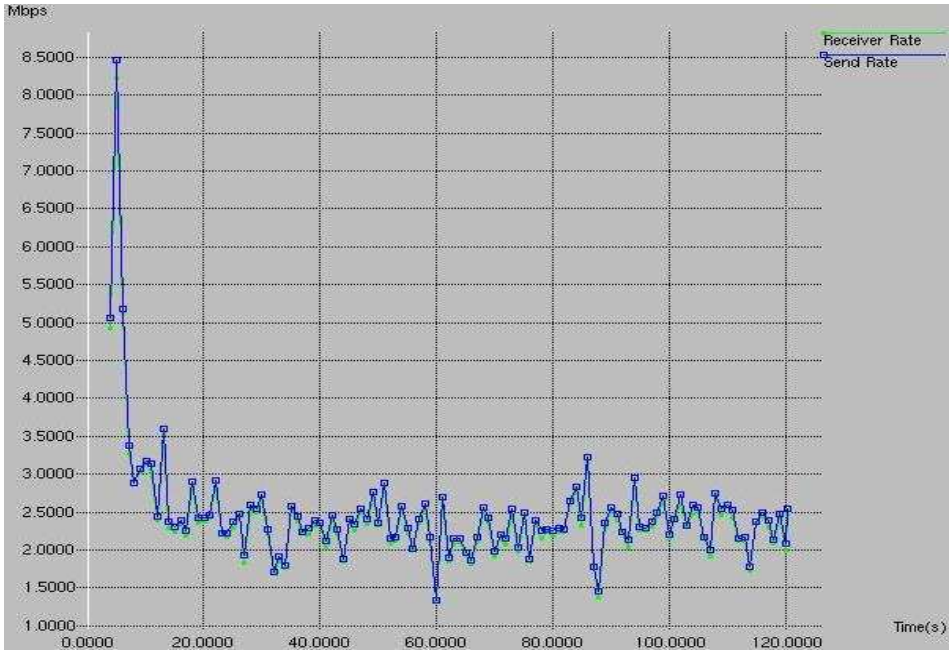


Figura 3.87: C2 (2,2M) PLATA a 3M

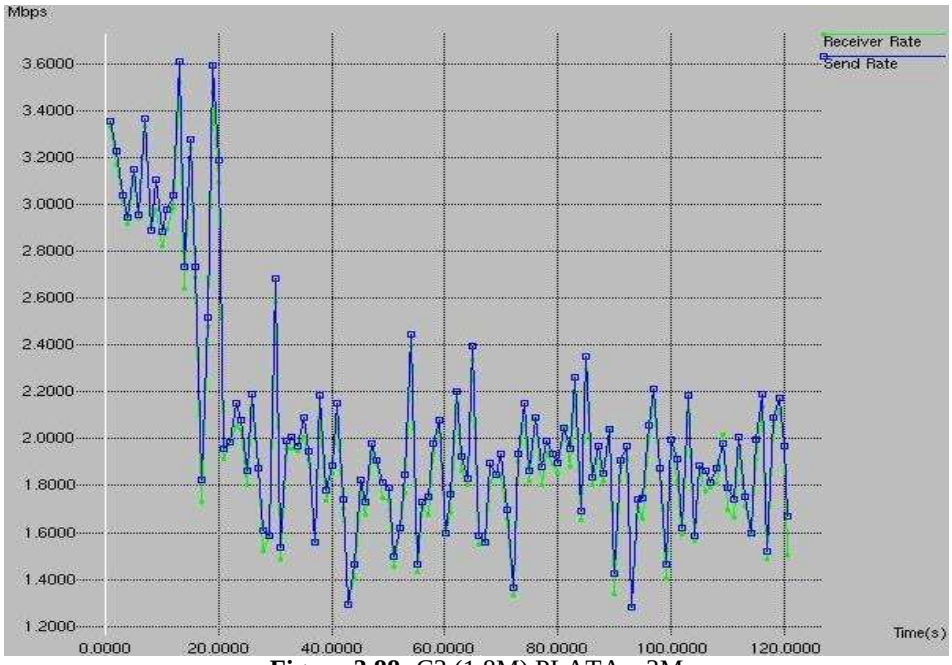


Figura 3.88: C3 (1,8M) PLATA a 3M

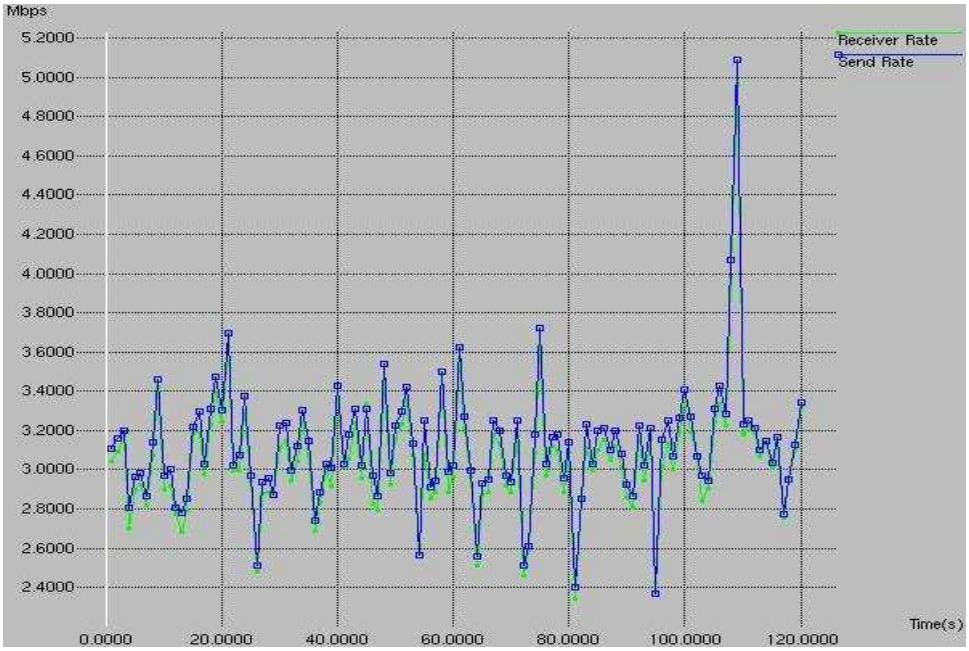


Figura 3.89: C4 (2,6M) PLATA a 3M

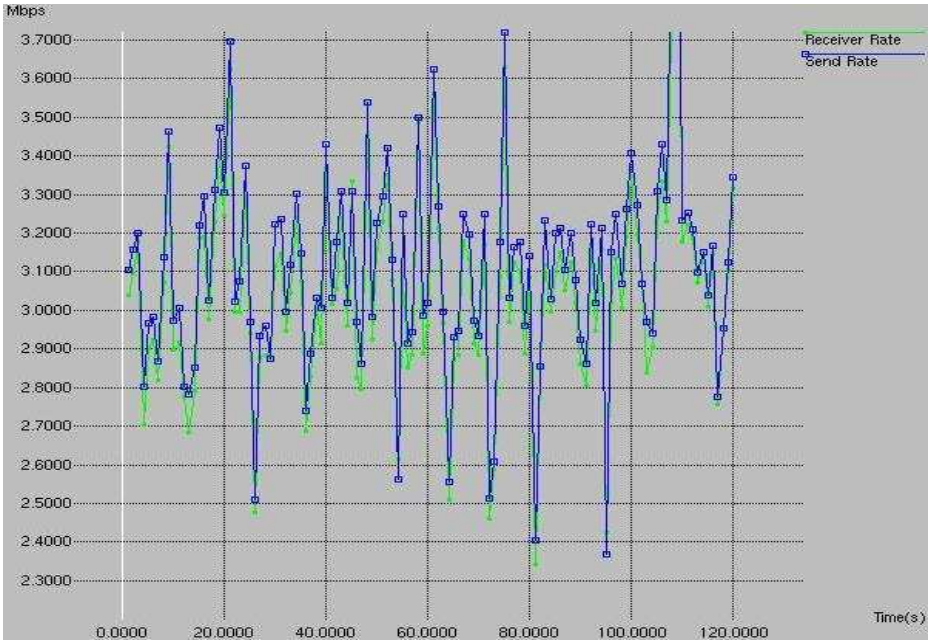


Figura 3.90: Zoom C4 (2,6M) PLATA a 3M

En este caso, todas las fuentes comienzan transmitiendo a 3M y por tanto se produce congestión. Todas las fuentes son TCP pero tienen distintos contratos. En las gráficas se observa que los clientes con menor contrato obtienen menor ancho de banda que los de mayor contrato. Todos los clientes excepto el cliente C4 reducen su ventana de transmisión al detectar congestión, ya que el cliente C4 es el que tiene mayor contrato 2,6M (valor cercano a los 3M a los que las fuentes generan tráfico). Comparando con las gráficas cuando **no se aplican servicios diferenciados**, ahora se tienen en cuenta los contratos y el reparto del ancho de banda es proporcional al ancho de banda contratado por cada cliente. El cliente C4 obtiene el ancho de banda al que transmite 3M, gracias a los descartes de paquetes de los clientes C1 y C3, los de menor contrato 1,4M y 1,8M,

que obtienen 0,5M menos cada uno que en el caso de no aplicar *DiffServ*, obteniendo en torno a 2M. El cliente C2 obtiene aproximadamente 2,5M del ancho de banda total del enlace final.

En la tabla de resultados 3.32, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.32: Resultados para todas las fuentes TCP a 3M "Distintos Contratos" DROP

Filter ID	Filter-PKTS	Filter-OCTETS	Ventana de transmisión	TRAFFIC PROFILE DISCARD PKTS	BW DESCARTADO	BW (Mbps)
1 (1,4M)	21877	32946574	2,196438	**2313**	0,1579	**2,038538**
3 (1,8M)	23149	35107774	2,340518	**2289**	0,156262	**2,184256**
4 (2,6M)	33726	49966988	3,331132	**1927**	0,131549	**3,199582**
2 (2,2M)	26659	39949402	2,663293	**2049**	0,139878	**2,523415**

Ahora se está en situación de congestión y cada cliente obtiene un ancho de banda distinto en función de su contrato.

El **descarte** de paquetes depende del contrato de cada cliente y de su ventana de transmisión. Es mayor cuanto menor sea el contrato de los clientes. El cliente C4 logra conservar el ancho de banda al que transmite tráfico 3M acosta del descarte de paquetes de los clientes C1 y C3. El contrato de C4 (2,6M) es cercano a 3M. Los contratos de los clientes C1 y C3 son de 1,4M y 1,8M respectivamente, valores que están muy por debajo de los 3M, por tanto sufren el mayor descarte de paquetes y obtienen el menor ancho de banda, 2,03M y 2,18M respectivamente. El cliente C2 tiene un contrato de 2,2M, valor que ya no se aleja tanto, obteniendo un ancho de banda de 2,5M.

ii. Tráfico generado UDP y TCP

En esta prueba, los **contratos** de las fuentes generadoras de tráfico **TCP** C2 y C4 son **mayores** que los contratos de las fuentes generadoras de tráfico **UDP** C1 y C3.

1. **Tráfico generado por cada cliente: 1,25 Mbps**

   Tráfico total generado: 1,25 * 4 = 5 Mbps, 50% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

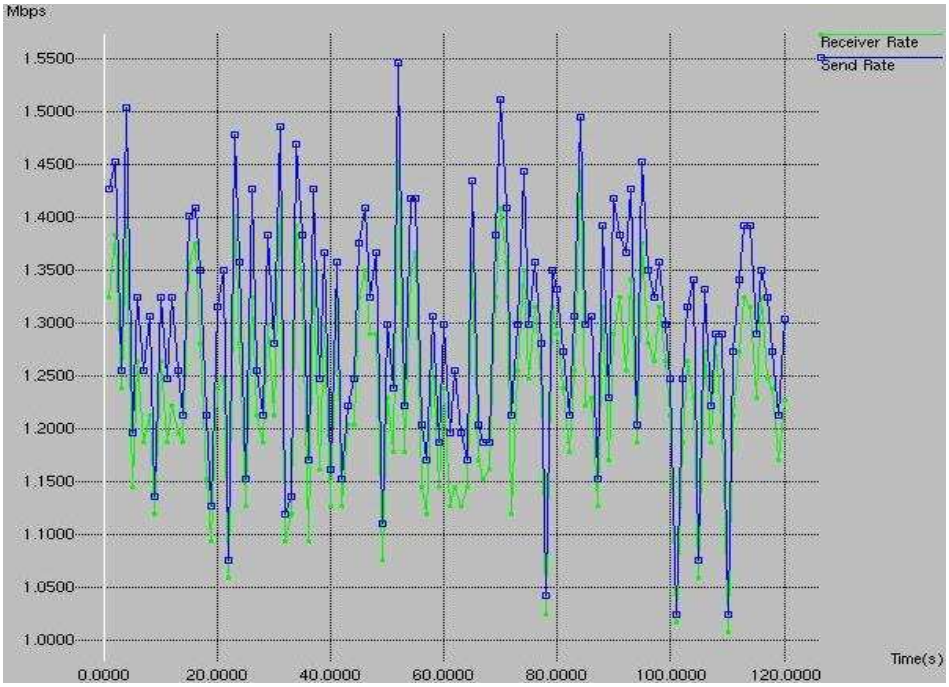


Figura 3.91: C1 (1,4M) UDP PLATA a 1,25M

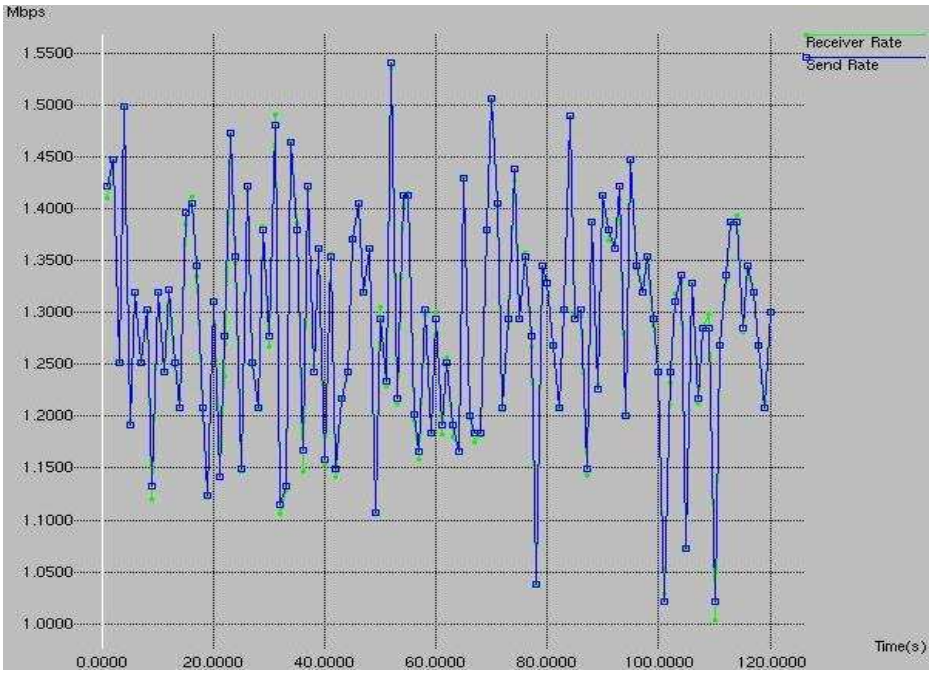


Figura 3.92: C2 (2,2M) TCP PLATA a 1,25M

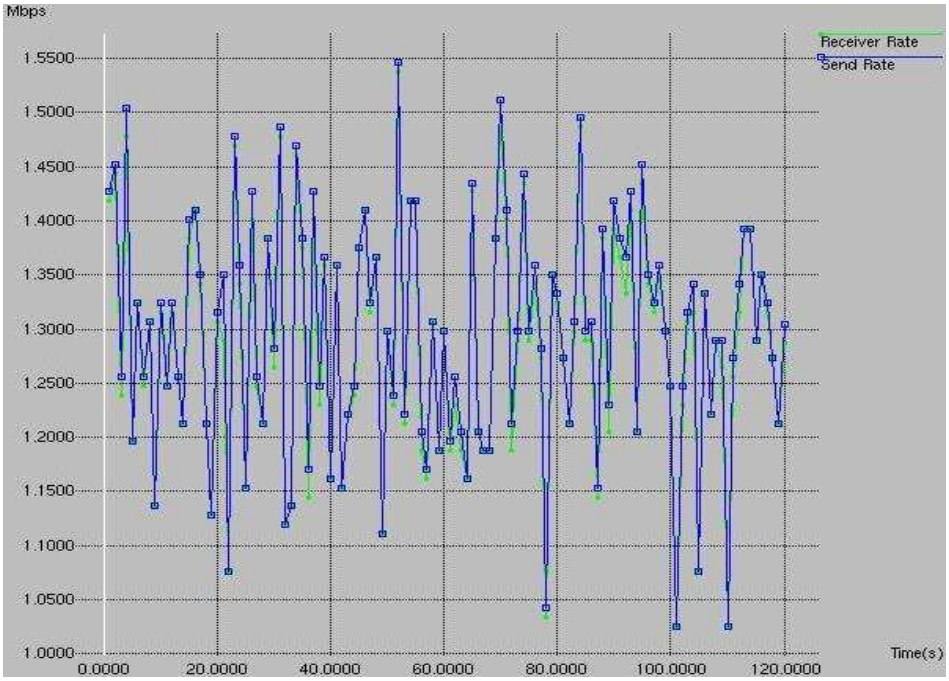


Figura 3.93: C3 (1,8M) UDP PLATA a 1,25M

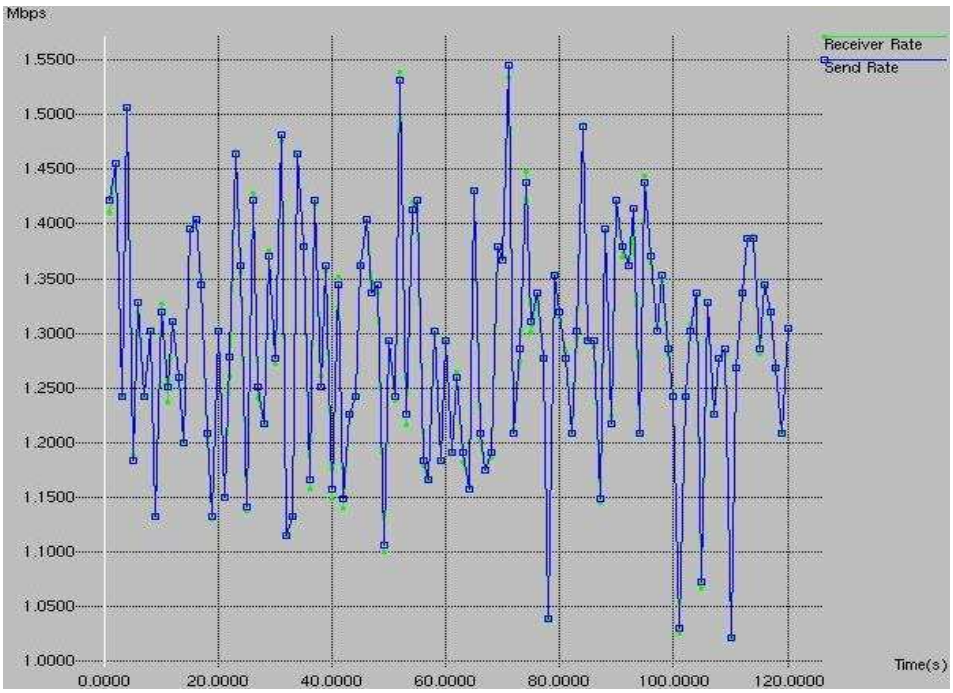


Figura 3.94: C4 (2,6M) TCP PLATA a 1,25M

En las gráficas se observa que conforme disminuye el contrato, mayor es la separación entre la línea azul y línea verde. Así, se deduce que el cliente C1 sufre más descartes de paquetes que el resto de las fuentes porque tiene mayor separación entre dichas líneas, pues es la fuente de menor contrato 1,4M. Aún así, la separación no es significativa pues todos los clientes cumplen su contrato y sobra ancho de banda. El descarte de paquetes se debe a que la transmisión de tráfico es en media.

En la tabla de resultados 3.33, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.33: Resultados para fuentes UDP y TCP a 1,25M "Distintos Contratos" DROP

Filter ID	Filter-PKTS	Filter-OCTETS	Ventana de transmisión	TRAFFIC PROFILE DISCARD PKTS	BW DESCARTADO	BW (Mbps)
UDP						
1 (1,4M)	18194	19540356	1,302690	**794**	0,054203	**1,248486**
3 (1,8M)	18194	19540356	1,302690	**115**	0,007850	**1,294839**
TCP						
4 (2,6M)	17641	19891426	1,326095	**21**	0,001433	**1,324661**
2 (2,2M)	17716	19946488	1,329765	**66**	0,004505	**1,32526**

Obtiene un mayor ancho de banda las fuentes TCP en torno a 1,32M, en las cuales el contrato es mayor. Aun así, el ancho de banda obtenido es prácticamente el mismo para todas las fuentes en torno a 1,3M, ya que no se está en situación de congestión y todos los clientes cumplen su contrato, por lo que cada cliente se lleva el ancho de banda al que genera tráfico.
El mayor descarte de paquetes se aprecia en el cliente C1 el cual tiene el menor contrato **y es además fuente UDP**, es decir, transmite a la tasa máxima. Los descartes de paquetes no son significativos, ya que es por generar tráfico en media, y no porque falte ancho de banda.

2. Tráfico generado por cada cliente: 2 Mbps

Tráfico total generado: 2 * 4 = 8 Mbps, 80% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

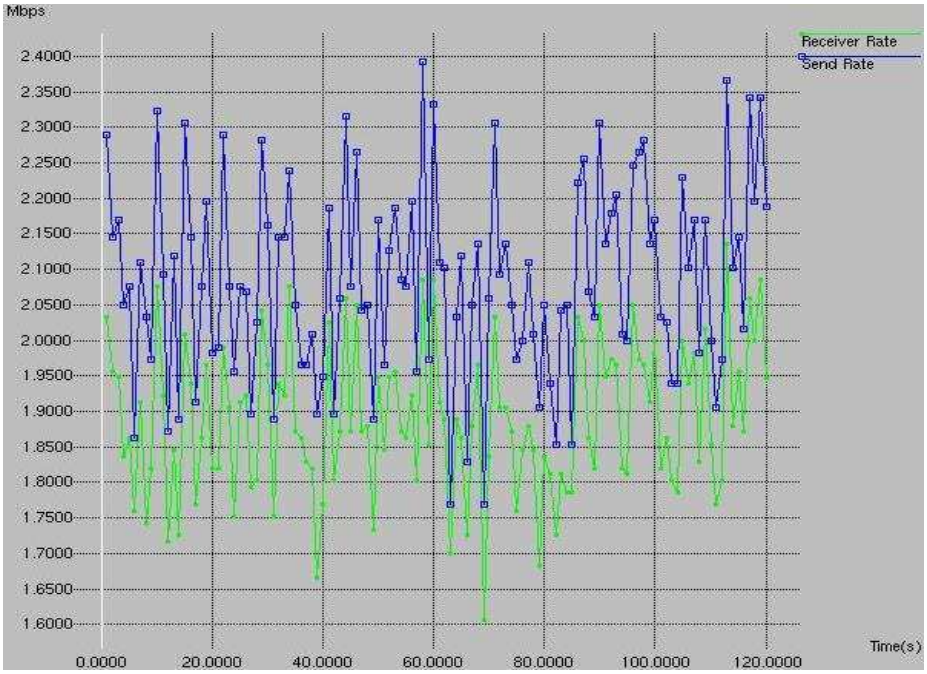


Figura 3.95: C1 (1,4M) UDP PLATA a 2M

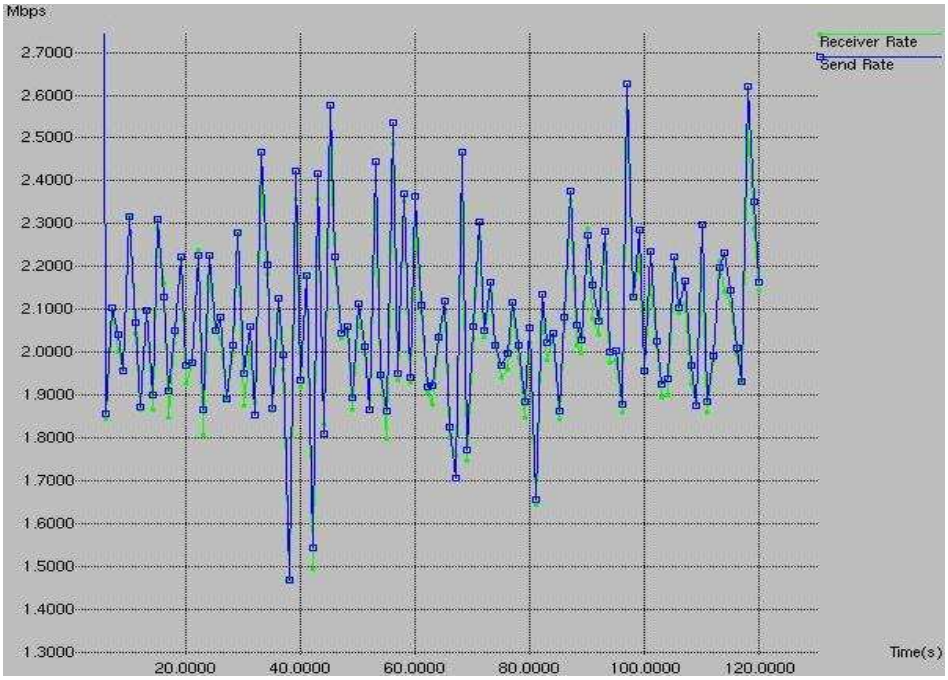


Figura 3.96: C2 (2,2M) TCP PLATA a 2M

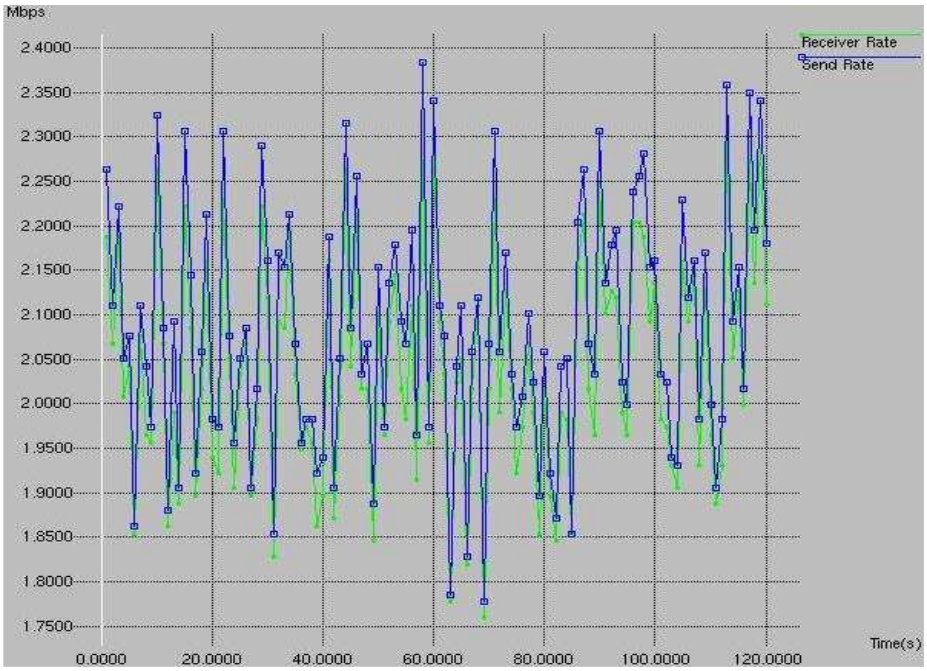


Figura 3.97: C3 (1,8M) UDP PLATA a 2M

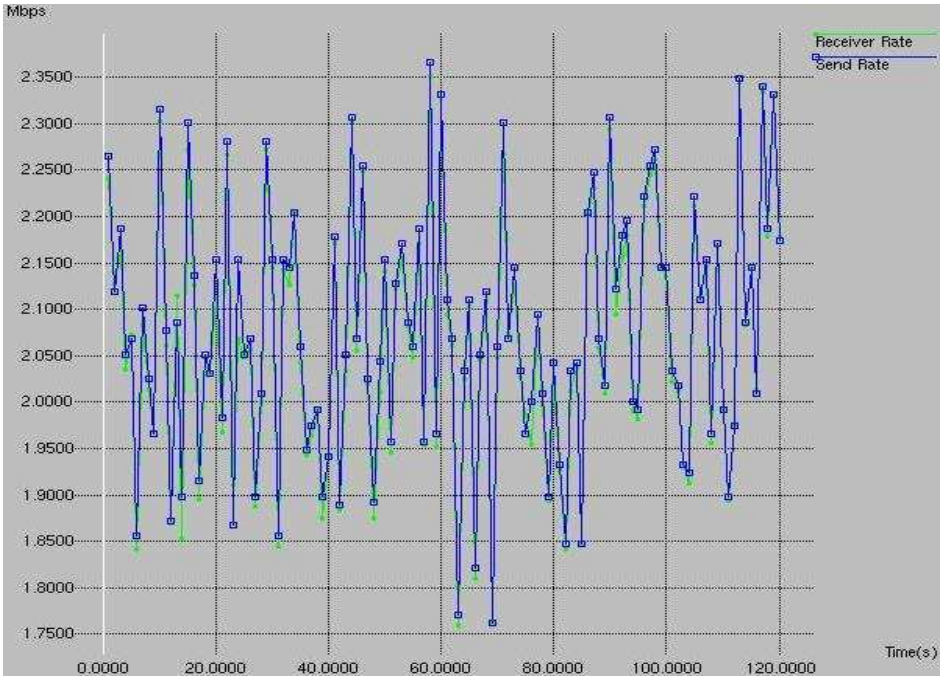


Figura 3.98: C4 (2,6M) TCP PLATA a 2M

En este escenario se ocupa el 80% del canal, con lo cual se está en el límite a partir del cual las prestaciones de la red comienzan a degradarse. Pasado este límite el tráfico UDP acapara los recursos frente al tráfico TCP.
Al aplicar Servicios Diferenciados, se observa que en las gráficas de tráfico UDP, clientes C1 y C3, la línea azul y la verde se separan ligeramente. Esto es debido a los descartes que sufre. La separación es mayor en el cliente C1 por tener menor contrato. Aún así, se obtiene el ancho de banda al que transmite, ya que **hay ancho de banda de sobra** para todas las fuentes.
Por otro lado, en las gráficas de tráfico TCP, clientes C2 y C4 se aprecia que la línea azul prácticamente coincide con la línea verde, con lo cual los clientes TCP obtienen el ancho de banda al que transmiten.

En la tabla de resultados 3.34, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.34: Resultados para fuentes UDP y TCP a 2M "Distintos Contratos" DROP

Filter ID	Filter-PKTS	Filter-OCTETS	Ventana de transmisión	TRAFFIC PROFILE DISCARD PKTS	BW DESCARTADO	BW (MBPS)
UDP						
1 (1,4M)	29252	31416648	2,094443	**2730**	0,186368	**1,908075**
3 (1,8M)	29254	31418796	2,094586	**598**	0,040823	**2,053763**
TCP						
4 (2,6M)	26439	32031066	2,135404	**188**	0,012834	**2,122570**
2 (2,2M)	25460	33504336	2,23d3622	**1340**	0,091477	**2,142145**

Al **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **2M** ya que el programa generador de tráfico *Traffic Generator* genera en media.

En las fuentes TCP, se observa que el cliente C4 por tener el mayor contrato sufre menor descarte de paquetes. El cliente TCP C2 a pesar de tener mayor contrato que el cliente UDP C3 sufre más descartes **debido al propio descarte**, ya que TCP detecta las pérdidas y **reenvía los paquetes descartados**. El mayor descarte de paquetes se aprecia en el C1 el cual tiene el menor contrato y **es además fuente UDP**, es decir, todo el tiempo transmite a la tasa máxima.

3. Tráfico generado por cada cliente: 3 Mbps

Tráfico total generado: 3 * 4 = 12 Mbps, 120% del ancho de banda total. Por tanto, se forma **cuello de botella en** el enlace final.

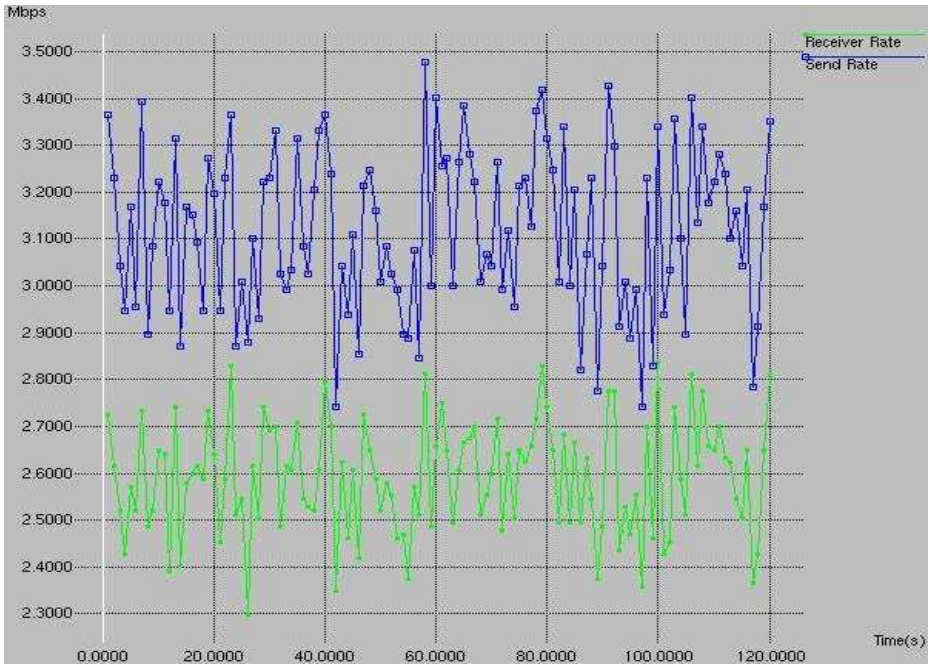


Figura 3.99: C1 (1,4M) UDP PLATA a 3M

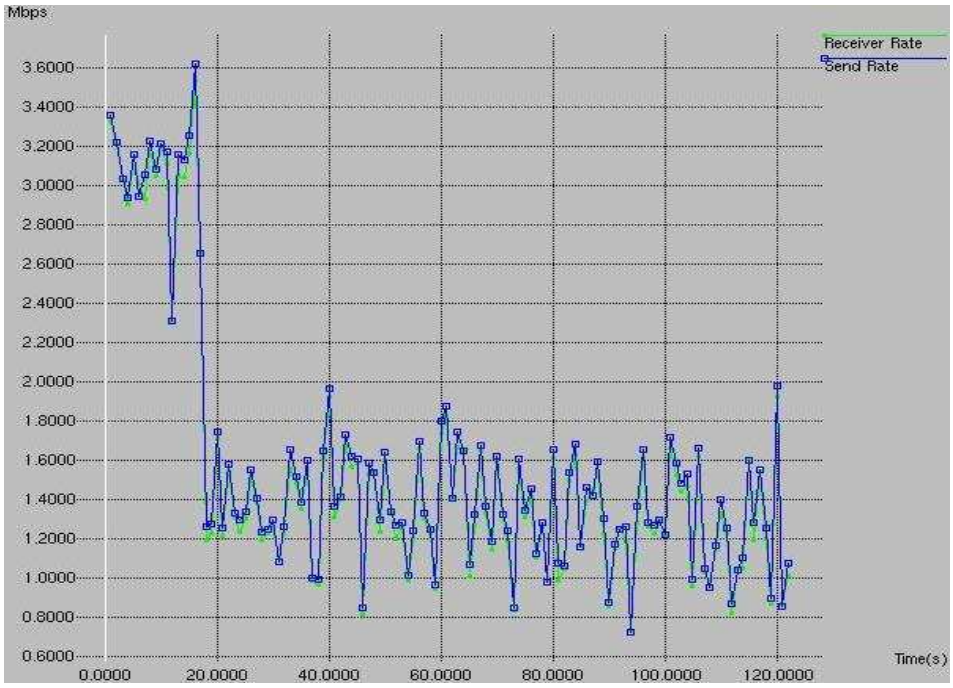


Figura 3.100: C2 (2,2M) TCP PLATA a 3M

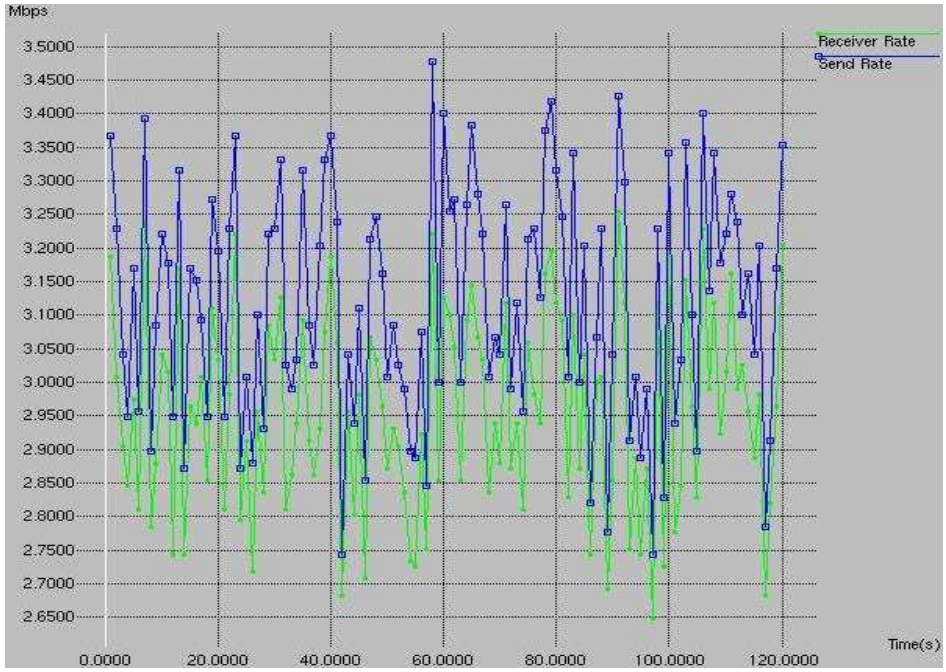


Figura 3.101: C3 (1,8M) UDP PLATA a 3M

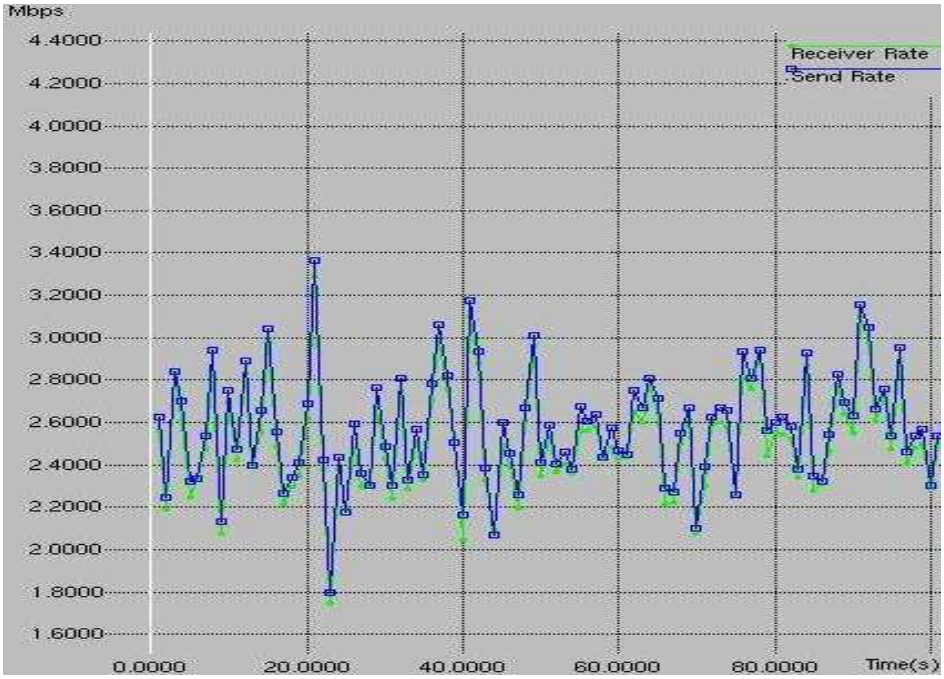


Figura 3.102: C4 (2,6M) TCP PLATA a 3M

En este caso, todas las fuentes comienzan transmitiendo a 3M y por tanto se produce congestión.
En las gráficas se observa que los clientes con menor contrato no obtienen el menor ancho de banda como cabría esperar. Así, el cliente C1, el de menor contrato (1,4M), obtiene en torno a 2,6M; y el cliente C3, de contrato (1,8M), obtiene prácticamente los 3M a los que transmite. Esto se debe a que en este escenario **se enfrenta tráfico TCP con tráfico UDP**. Las fuentes UDP no se enteran de la congestión por lo que **no reducen su ventana de transmisión**, por lo que intentan transmitir a 3M todo el tiempo, es decir, acaparar todos los recursos.
Al **aplicar Servicios Diferenciados**, la fuente UDP con menor contrato C1 sufre una disminución de 0,5M respecto al ancho de banda al que transmite, y la fuente TCP C2 detecta la congestión y reduce bruscamente su ventana de transmisión de 3M a unos **1,7M**. Gracias a esta reducción y al descarte de paquetes en la fuente UDP C1, el cliente TCP C4 puede mantener su ventana de transmisión y obtener los 3M a los que transmite tráfico. El cliente C4 es el que tiene mayor contrato 2,6M (valor cercano a los 3M a los que las fuentes generan tráfico).
En las gráficas el descarte de paquetes se traduce en la separación entre la línea azul y la línea verde, cuanto mayor es la separación mayor es el descarte. En la gráfica del cliente UDP C1 al tener el menor contrato y por ser fuente UDP se aprecia la mayor separación entre la línea azul y la línea verde, esto es, es el que sufre mayor descarte de paquetes.
Comparando con las gráficas cuando **no se aplican servicios diferenciados**, ahora se tienen en cuenta **los contratos** y **el tipo de tráfico** UDP o TCP para el reparto del ancho de banda no contratado.

En la tabla de resultados 3.35, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.35: Resultados para fuentes UDP y TCP a 3M "Distintos Contratos" DROP

Filter ID	Filter-PKTS	Filter-OCTETS	Ventana de transmisión	TRAFFIC PROFILE DISCARD PKTS	BW DESCARTADO	BW (Mbps)
UDP						
1 (1,4M)	43794	47034756	3,13565	**7508**	0,512546	**2,623104**
3 (1,8M)	43794	47034756	3,13565	**2272**	0,155101	**2,980548**
TCP						
4 (2,6M)	31581	47593710	3,172914	**478**	0,032578	**3,140336**
2 (2,2M)	17472	26210216	1,747347	**1821**	0,124313	**1,623034**

Ahora se está en situación de congestión y cada cliente obtiene un ancho de banda distinto en función de su contrato y el tipo de tráfico UDP o TCP.

El **descarte** de paquetes depende del contrato de cada cliente, de su ventana de transmisión y del tipo de tráfico que se transmita UDP o TCP. Es mayor cuanto menor sea el contrato de los clientes. Obtiene un **mayor ancho de banda las fuentes UDP** ya que éstas no reducen su ventana de transmisión pero se descartan mayor número de paquetes que en las fuentes TCP, por tener menor contrato y no reducir su ventana de transmisión. El cliente UDP C1 cuyo contrato es el menor, obtiene **2,6M** perdiendo un ancho de banda de 0,5M. El cliente UDP C3 consigue prácticamente los 3M a los que transmite. El cliente TCP C2 reduce drásticamente su ventana de transmisión, logrando sólo **1,62M** del ancho de banda total del enlace final, y así el cliente TCP C4 puede mantener su ventana de transmisión (3M). Además, el cliente C4 logra conservar el ancho de banda al que transmite tráfico 3M acosta del descarte de paquetes del cliente UDP C1.

3.3.3.2 Caso Plata-Oro: configuración con dos colas y distintos contratos

3.3.3.2.1 Sin aplicar Servicios Diferenciados (sin activar DROP)

- Prueba **contratos C2 y C4 TCP > contratos C1 y C3 UDP**

  En esta prueba, los contratos de las fuentes generadoras de tráfico TCP C2 y C4 son mayores que los contratos de las fuentes generadoras de tráfico UDP C1 y C3.

  1. **Tráfico generado por cada cliente: 1,25 Mbps**

     Tráfico total generado: 1,25 * 4 = 5 Mbps, 50% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

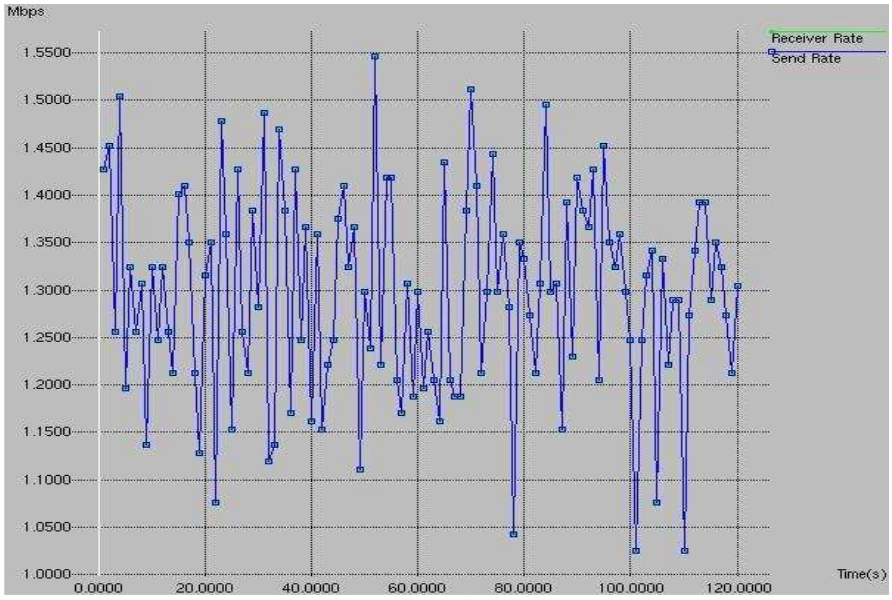


Figura 3.103: C1 (1,4M) UDP ORO a 1,25M

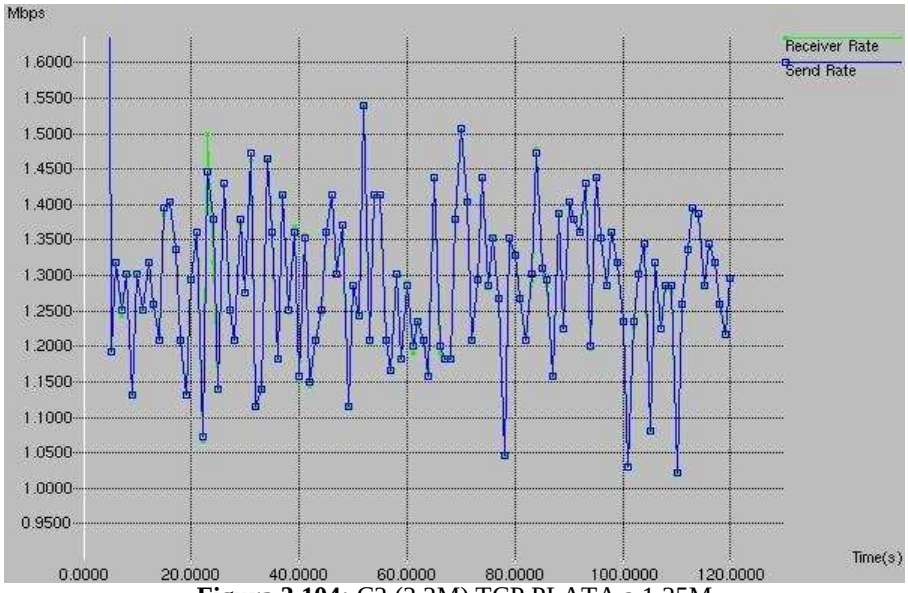


Figura 3.104: C2 (2,2M) TCP PLATA a 1,25M

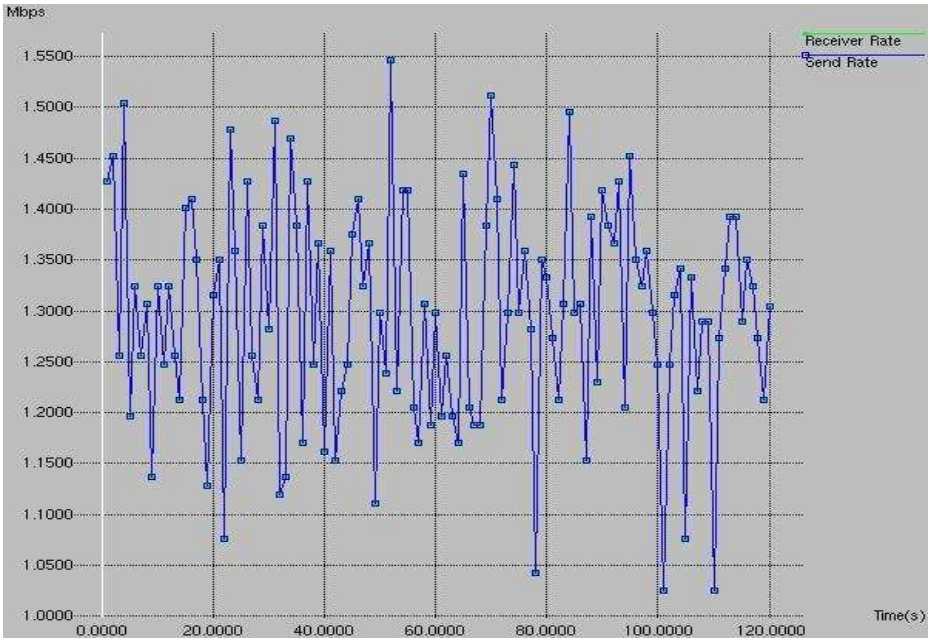


Figura 3.105: C3 (1,8M) UDP PLATA a 1,25M

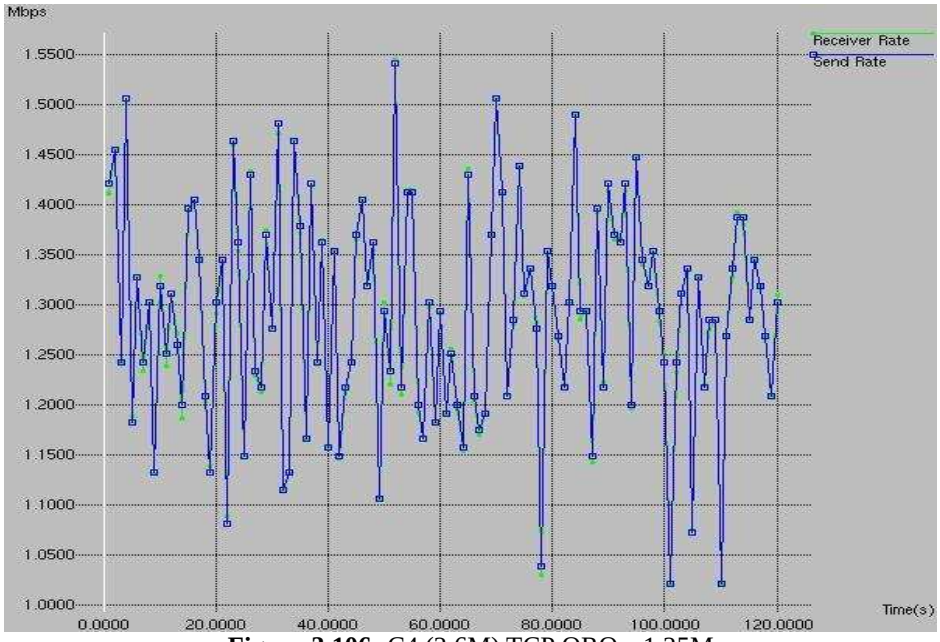


Figura 3.106: C4 (2,6M) TCP ORO a 1,25M

En todas las gráficas se observa que la línea azul coincide con la línea verde, con lo cual todos los clientes obtienen el ancho de banda al que transmiten, en torno a 1,3M.

En la tabla de resultados 3.36, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.36: Resultados para fuentes UDP y TCP a 1,25M "Distintos Contratos" dos colas

Filter ID	Filter- PKTS	Filter-OCTETS	TRAFFIC PROFILE DISCARD PKTS	BW (Mbps)	
UDP					
1 (1,4M)	18194	19540356	0	1,30269	**ORO**
3 (1,8M)	18194	19540356	0	1,30269	**PLATA**
TCP					
4 (2,6M)	17651	19866234	0	1,324415	**ORO**
2 (2,2M)	17528	19857632	0	1,323842	**PLATA**

Todos los clientes obtienen el mismo ancho de banda.
Al **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **1,3M**.

Nota: La ventana de transmisión **no se ajusta perfectamente a 1,25 Mbps**, ya que el programa *Traffic Generator* transmite en media.

2. Tráfico generado por cada cliente: 2 Mbps

Tráfico total generado: 2 * 4 = 8 Mbps, 80% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

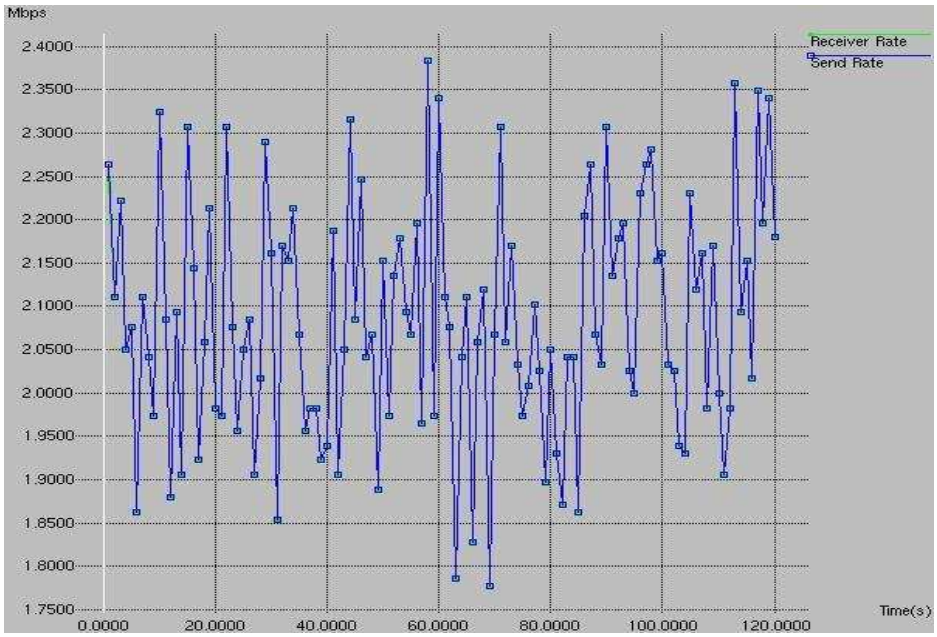


Figura 3.107: C1 (1,4 M) UDP ORO a 2M

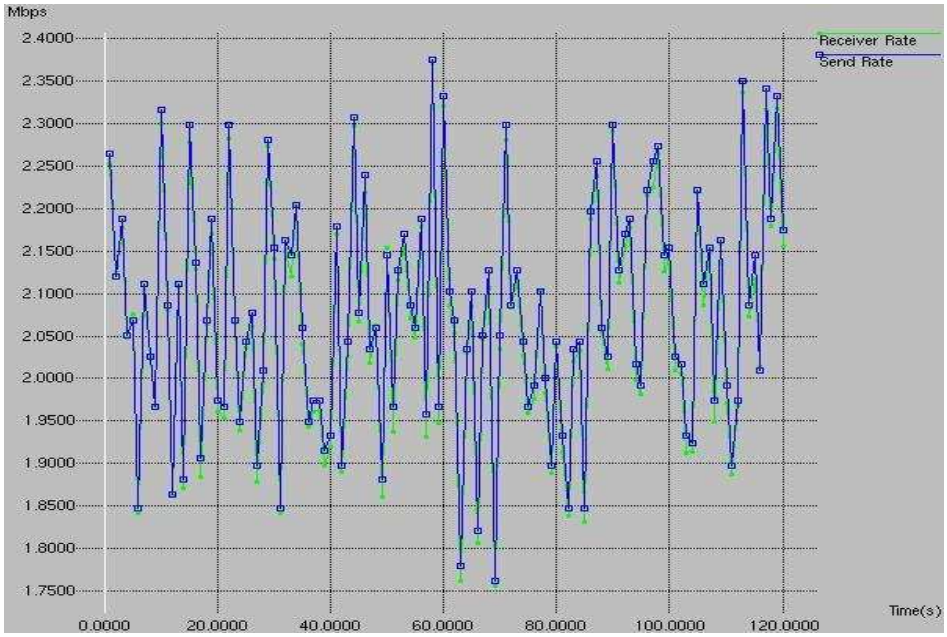


Figura 3.108: C2 (2,2 M) TCP PLATA a 2M

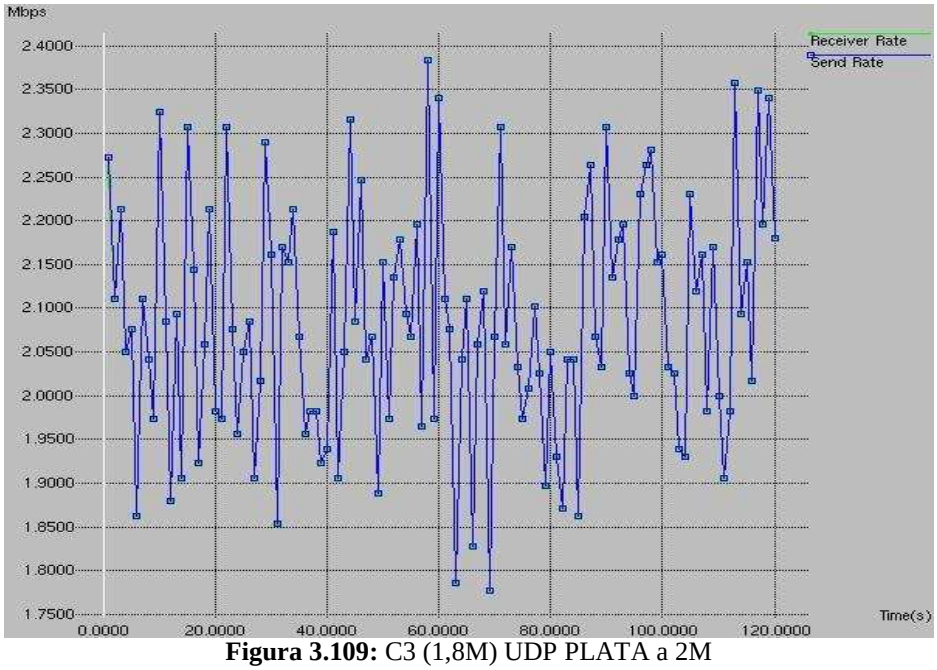


Figura 3.109: C3 (1,8M) UDP PLATA a 2M

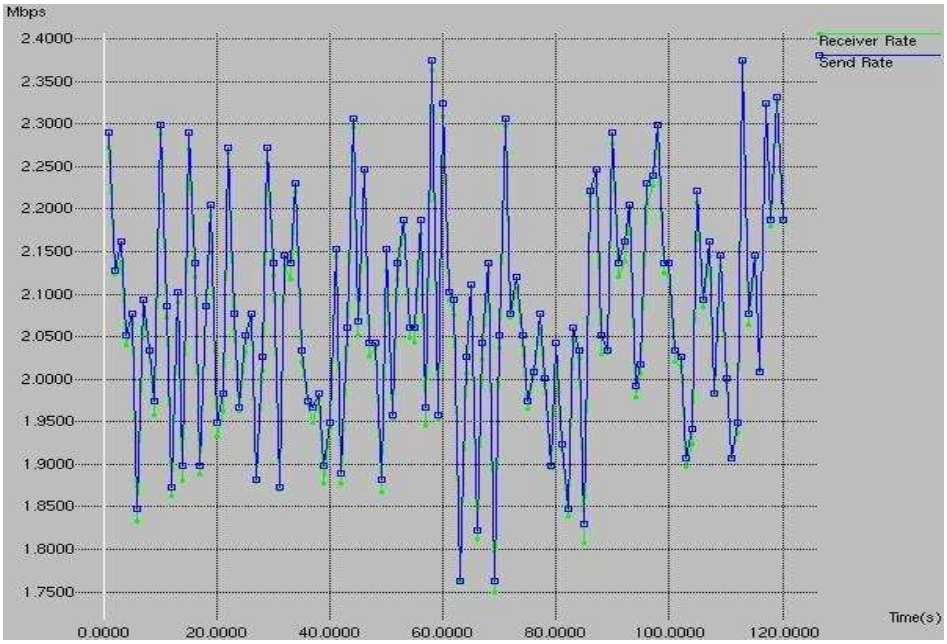


Figura 3.110: C4 (2,6M) TCP ORO a 2M

En este escenario se ocupa el 80% del canal, con lo cual se está en el límite a partir del cual las prestaciones de la red comienzan a degradarse. Pasado este límite el tráfico UDP acapara los recursos frente al tráfico TCP.

Por un lado, se observa, que en las gráficas de tráfico UDP, clientes C1 y C3, la línea azul coincide perfectamente con la línea verde, es decir, transmiten a la tasa máxima, con lo cual los clientes UDP obtienen el ancho de banda al que transmiten.

Por otro lado, en las gráficas de tráfico TCP, clientes C2 y C4 se aprecia que la línea azul prácticamente coincide con la línea verde, con lo cual se puede decir que los clientes TCP obtienen el ancho de banda al que transmiten. La diferencia con las gráficas de tráfico UDP, es que en las de tráfico TCP se distinguen picos verdes ligeramente por debajo de la línea azul, esto es debido a que se genera tráfico en media y cuando se enfrenta tráfico UDP frente a TCP, el UDP no colabora, es decir, no reduce su ventana de transmisión y continúa transmitiendo a la tasa máxima.

En la tabla de resultados 3.37, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.37: Resultados para fuentes UDP y TCP a 2M "Distintos Contratos" dos colas

Filter ID	Filter- PKTS	Filter-OCTETS	TRAFFIC PROFILE DISCARD PKTS	BW (Mbps)	
UDP					
1 (1,4M)	29252	31416648	0	2,094443	**ORO**
3 (1,8M)	29252	31416648	0	2,094443	**PLATA**
TCP					
4 (2,6M)	25170	31718004	0	2,114533	**ORO**
2 (2,2M)	25145	31716254	0	2,114416	**PLATA**

Todos los clientes obtienen el mismo ancho de banda.
Al **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **2,1M**.

Nota: el programa generador *Traffic Generator* genera tráfico en media.

3. **Tráfico generado por cada cliente: 3 Mbps**

   Tráfico total generado: 3 * 4 = 12 Mbps, 120% del ancho de banda total. Por tanto, se forma **cuello de botella en** el enlace final.

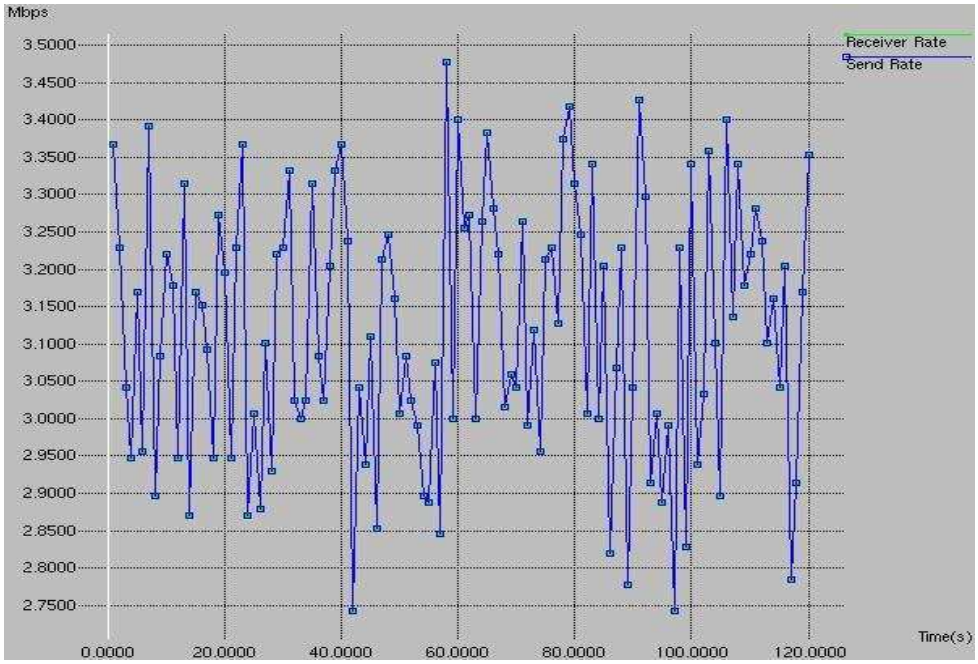


Figura 3.111: C1 (1,4 M) UDP ORO a 3M

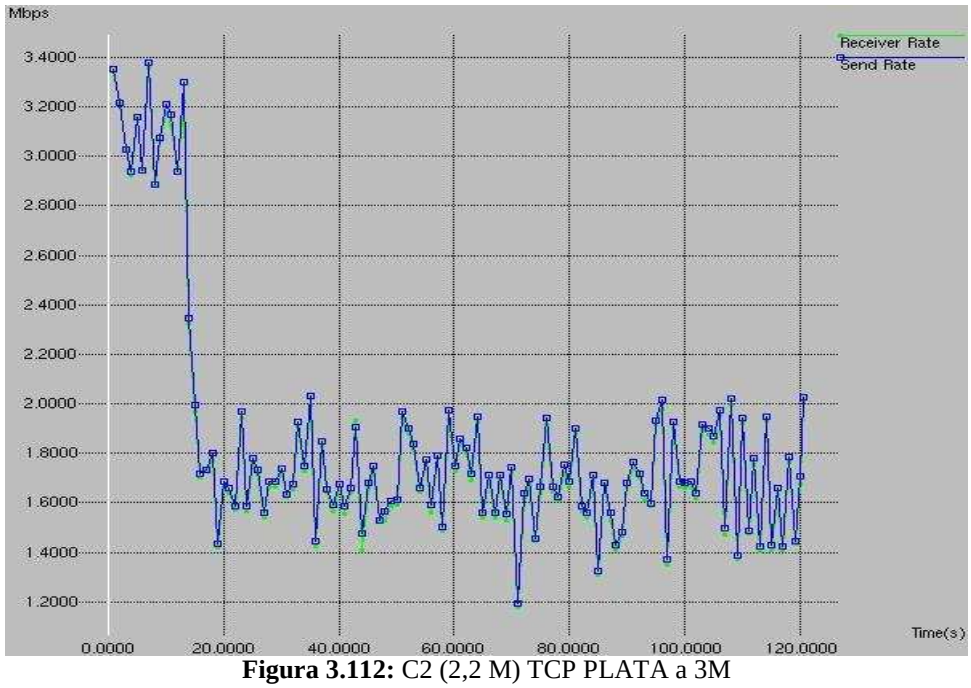


Figura 3.112: C2 (2,2 M) TCP PLATA a 3M

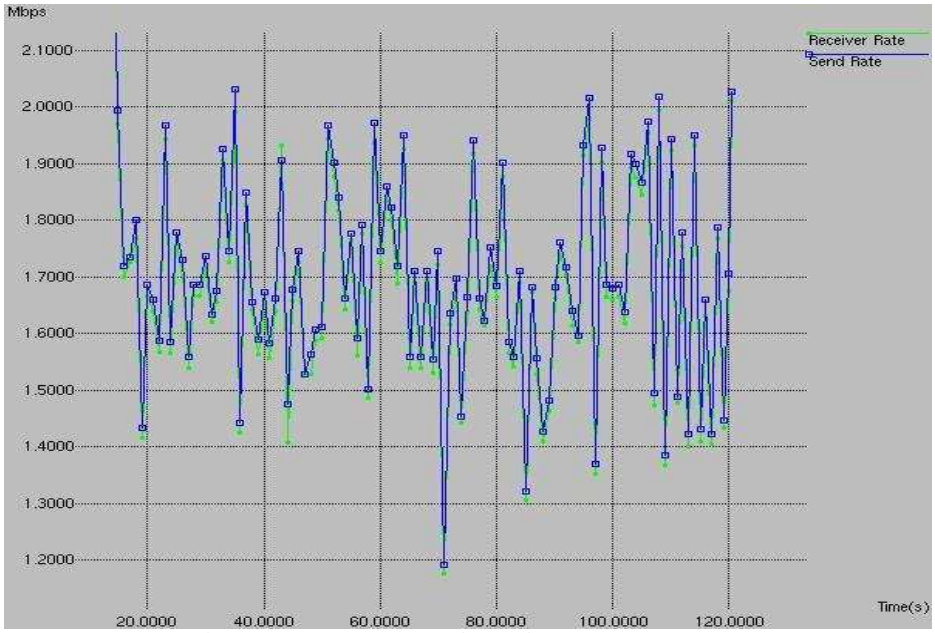


Figura 3.113: Zoom C2 (2,2 M) TCP PLATA a 3M

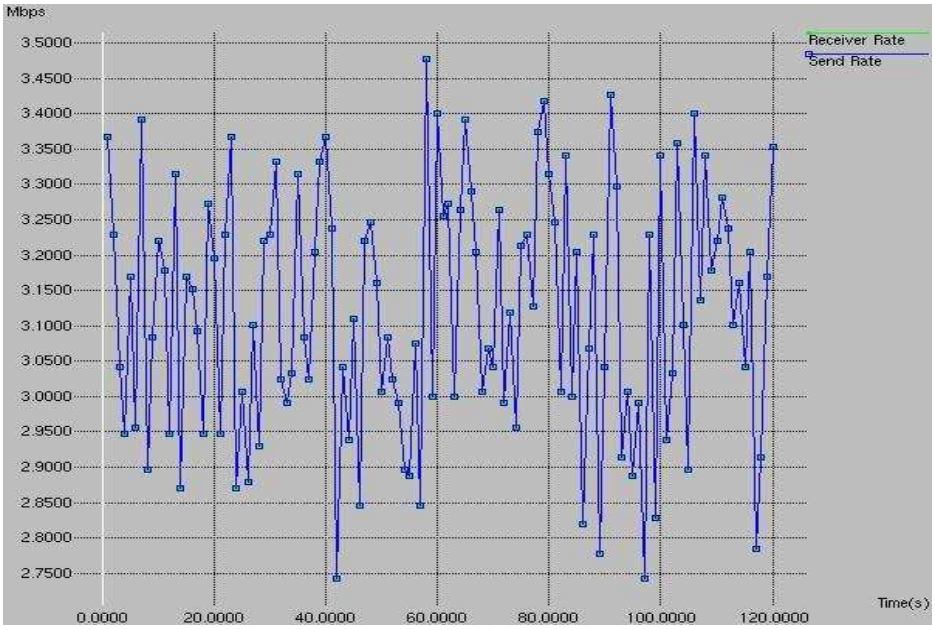


Figura 3.114: C3 (1,8M) UDP PLATA a 3M

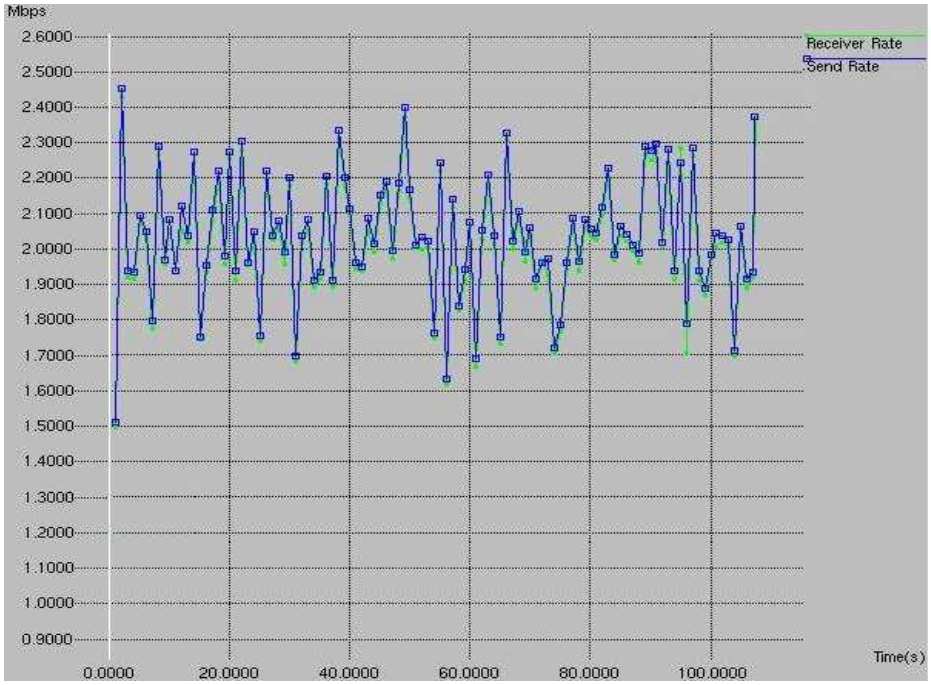


Figura 3.115: C4 (2,6M) TCP ORO a 3M

En las gráficas de tráfico TCP, clientes C2 y C4, se observa que la línea azul queda ligeramente por encima de la línea verde, ya que en este caso al estar en **situación de congestión** las fuentes TCP no obtienen el ancho de banda máximo al que transmiten.
Los **clientes UDP**, clientes C1 y C3, consiguen los 3M a los que generan tráfico, puesto que las fuentes UDP no se enteran de la congestión y continuarán transmitiendo a la tasa máxima. Del ancho de banda total sobran 2M para cada cliente TCP. En este escenario con dos colas, las fuentes TCP reducen su ventana de transmisión de modo que se reparten el sobrante en función de su **prioridad**. Así, el C2 reduce más su ventana de transmisión que el C4 (el cual tiene mayor prioridad).
Se observa como en un principio el **cliente TCP C2** comienzan a generar tráfico a 3M hasta detectar la congestión, entonces reduce su ventana de transmisión. El **cliente TCP C4**, al empezar a transmitir más tarde, directamente transmite a la ventana de transmisión (2,24M) que le corresponde en esta situación de congestión.

En la tabla de resultados 3.38, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.38: Resultados para fuentes UDP y TCP a 3M "Distintos Contratos" dos colas

Filter ID	Filter- PKTS	Filter-OCTETS	TRAFFIC PROFILE DISCARD PKTS	BW (Mbps)	
UDP					
1 (1,4M)	43796	47036904	0	3,135793	**ORO**
3 (1,8M)	43796	47036904	0	3,135793	**PLATA**
TCP					
4 (2,6M)	22441	33630710	0	2,242047	**ORO**
2 (2,2M)	19571	28184330	0	1,878955	**PLATA**

Al estar en situación de congestión, el tráfico UDP va a conseguir el ancho de banda al que genera tráfico, es decir, los clientes C1 y C3 consiguen un total de aproximadamente 6M del ancho de banda total, quedando alrededor de 4M a repartir entre los clientes C2 y C4.
Al existir dos colas de prioridad, el reparto del ancho de banda (4M) entre los **clientes TCP**, C2 y C4, no es equitativo, sino que depende del peso de cada cola. Así el cliente C4 obtiene mayor ancho de banda (2,24M) pues tiene mayor prioridad de emisión (cola Oro) que el cliente C2 el cual obtiene un ancho de banda de 1,8M (cola Plata).

INTERCAMBIO DE CONTRATOS

Tabla 3.39: Tasas contratadas para la configuración "Distintos Contratos" TCP<UDP

Id Filtro	**Clientes**	**Contrato**	**Valores "AverageRate"**
2	C2	1,4 M	27
4	C4	1,8 M	34
		3,2 M	
		40% de 8 M 32% de 10 M	
1	C1	2,2 M	42
3	C3	2,6 M	50
		4,8M	
		60% de 8 M 48% de 10M	
Ancho de Banda Total Contratado		8 M	
Ancho de Banda del enlace final		10 M	
Ancho de Banda en exceso (no contratado)		**2 M**	

- Prueba **contratos C2 y C4 TCP < contratos C1 y C3 UDP**

  En esta prueba, los contratos de las fuentes generadoras de tráfico TCP C2 y C4 son **menores** que los contratos de las fuentes generadoras de tráfico UDP C1 y C3.

1. **Tráfico generado por cada cliente: 1,25 Mbps**

   Tráfico total generado: 1,25 * 4 = 5 Mbps, 50% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

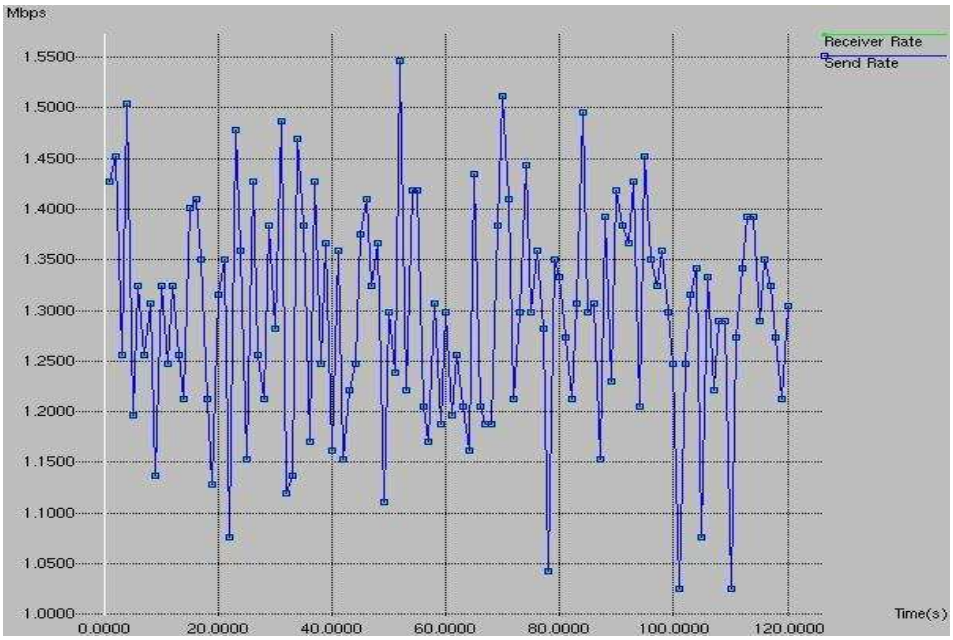


Figura 3.116: C1 (2,2 M) UDP ORO a 1,25M

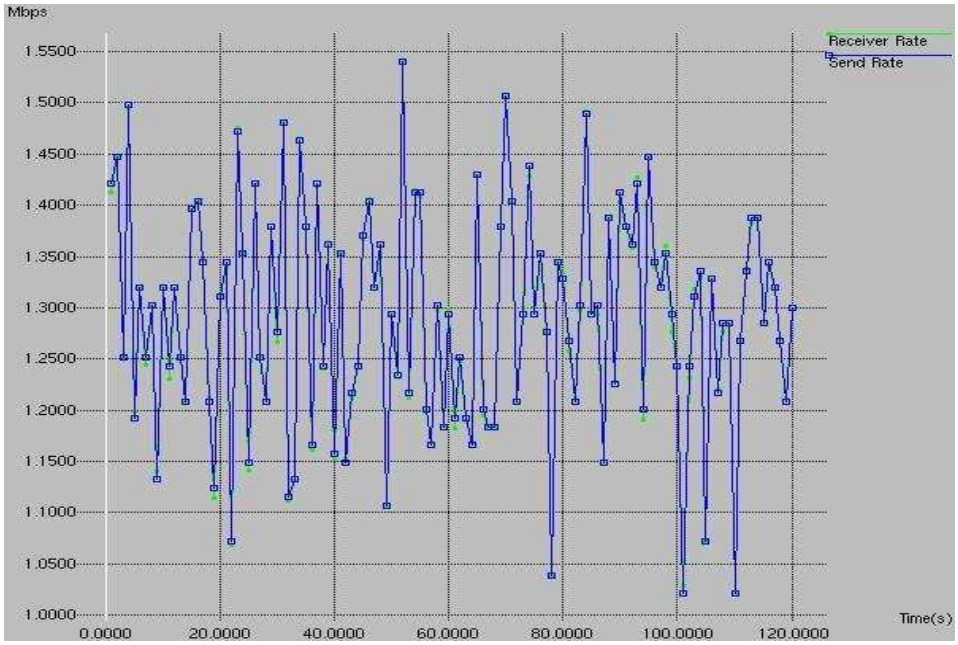


Figura 3.117: C2 (1,4 M) TCP PLATA a 1,25M

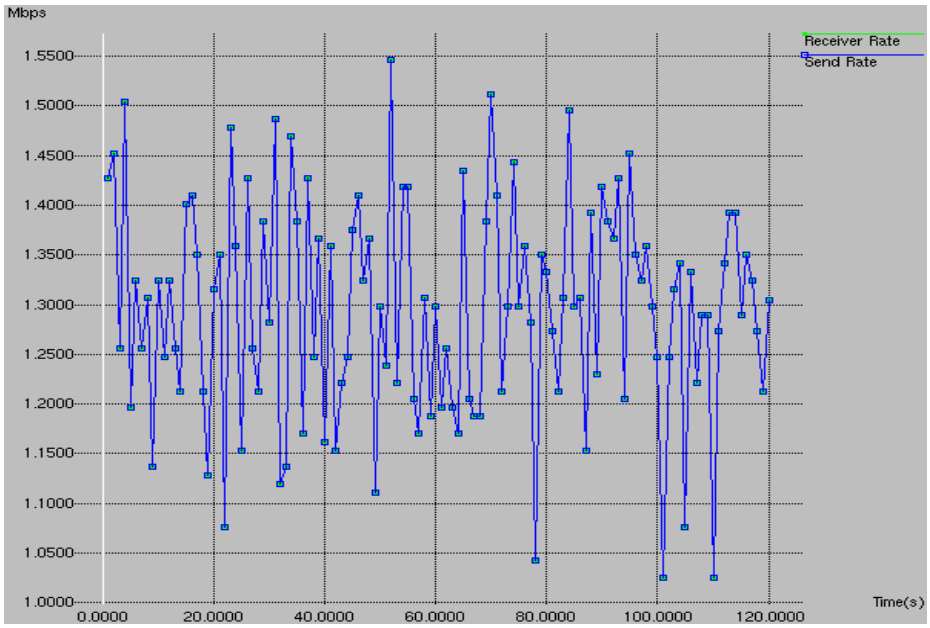


Figura 3.118: C3 (2,6 M) UDP PLATA a 1,25M

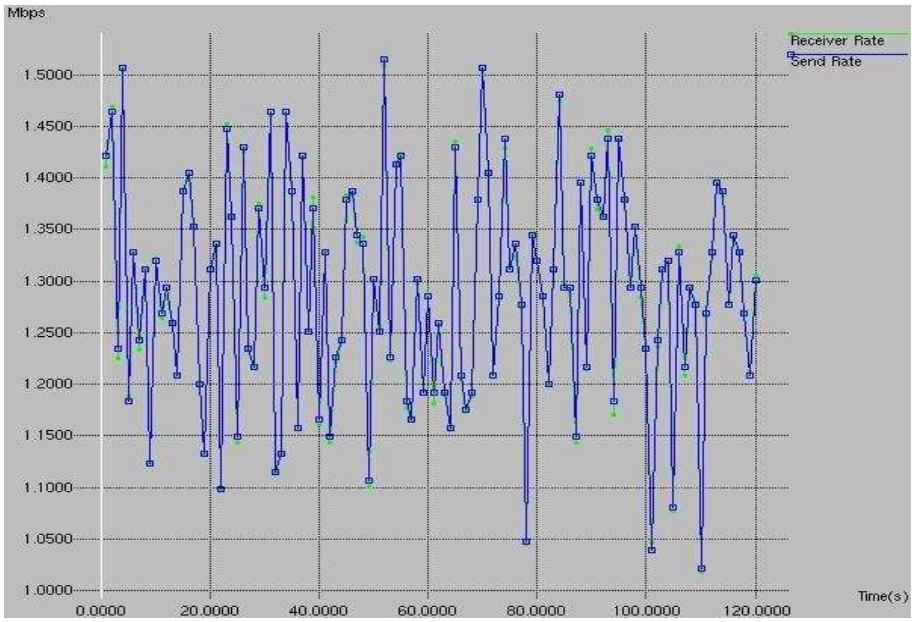


Figura 3.119: C4 (1,8 M) TCP ORO a 1,25M

En todas las gráficas se observa que la línea azul coincide con la línea verde, con lo cual todos los clientes obtienen el ancho de banda al que transmiten.

En la tabla de resultados 3.40, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.40: Resultados para fuentes UDP y TCP a 1,25M "Distintos Contratos" dos colas

Filter ID	Filter- PKTS	Filter-OCTETS	TRAFFIC PROFILE DISCARD PKTS	BW (Mbps)	
UDP 1 (2,2M) 3 (2,6M)	 18194 18194	 19540356 19540356	 0 0	 1,30269 1,30269	 **ORO** **PLATA**
TCP 4 (1,8M) 2 (1,4M)	 17645 17676	 19865814 19880168	 0 0	 1,324387 1,325344	 **ORO** **PLATA**

Todos los clientes obtienen el mismo ancho de banda.
Al **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **1,3M**.

Nota: La ventana de transmisión **no se ajusta perfectamente a 1,25 Mbps**, ya que el programa *Traffic Generator* transmite en media.

2. Tráfico generado por cada cliente: 2 Mbps

Tráfico total generado: 2 * 4 = 8 Mbps, 80% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

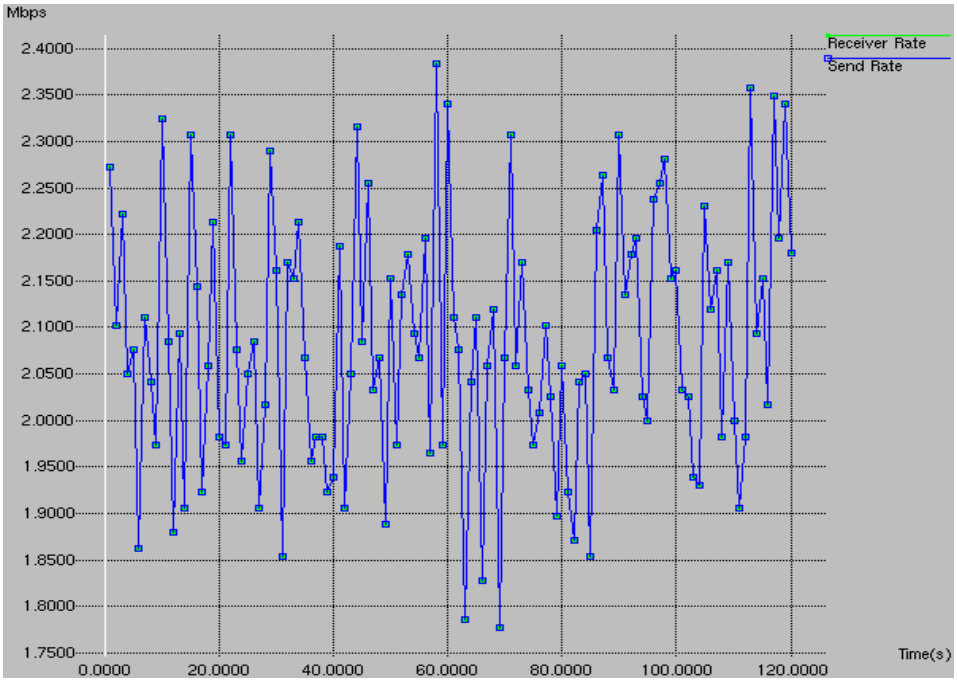


Figura 3.120: C1 (2,2 M) UDP ORO a 2M

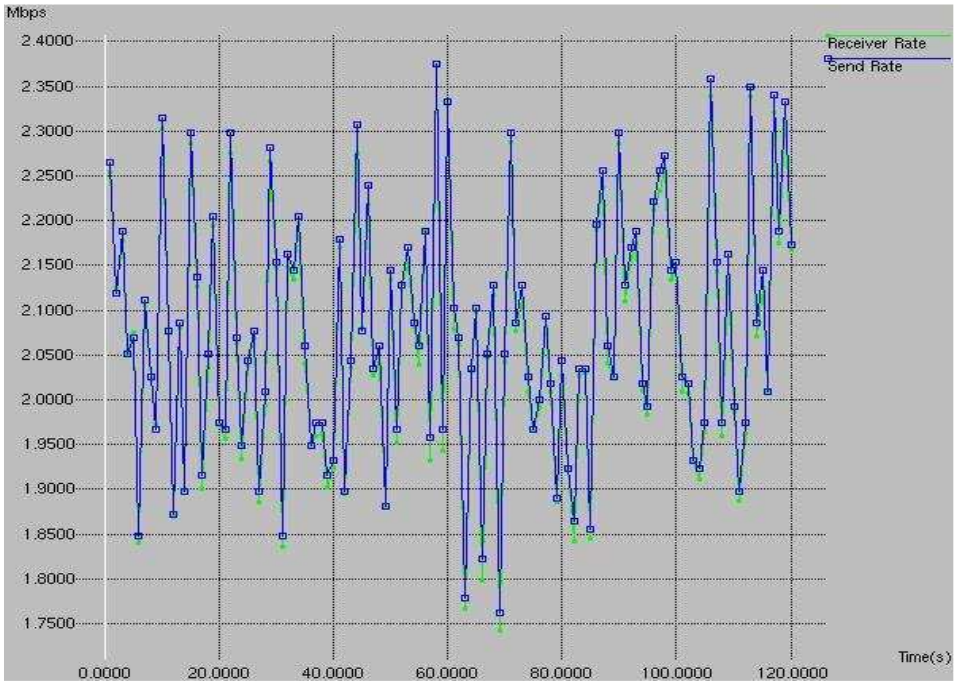


Figura 3.121: C2 (1,4 M) TCP PLATA a 2M

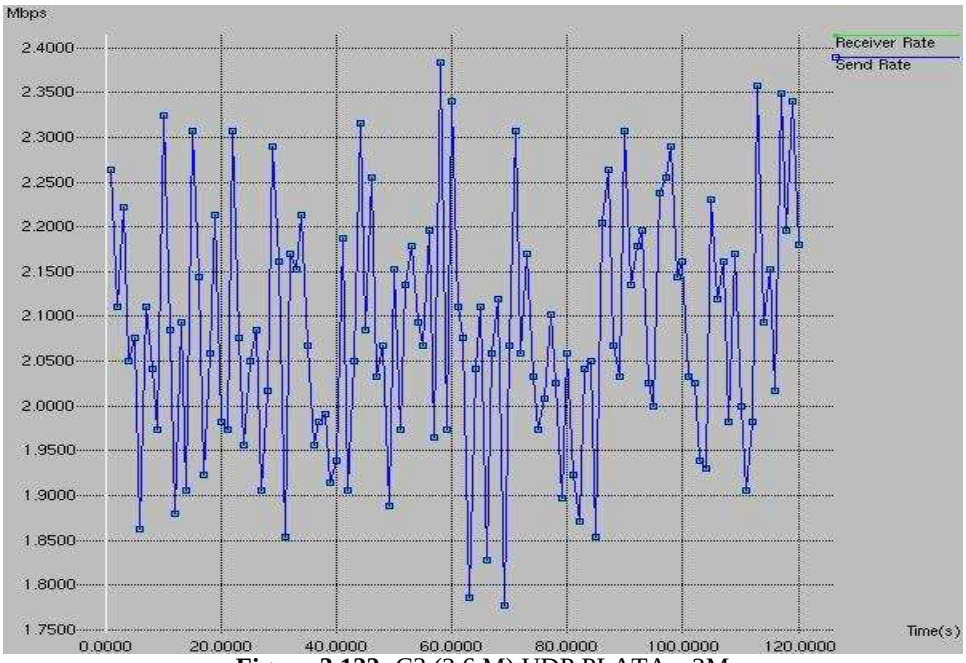


Figura 3.122: C3 (2,6 M) UDP PLATA a 2M

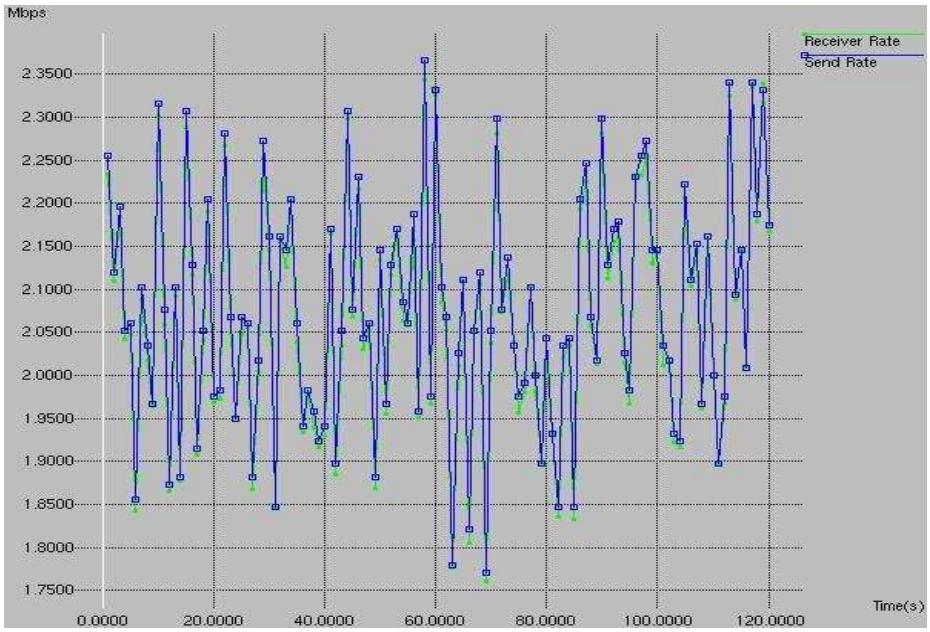


Figura 3.123: C4 (1,8 M) TCP ORO a 2M

En este escenario se ocupa el 80% del canal, con lo cual se está en el límite a partir del cual las prestaciones de la red comienzan a degradarse. Pasado este límite el tráfico UDP acapara los recursos frente al tráfico TCP.

Se observa, por un lado, que en las gráficas de tráfico UDP, clientes C1 y C3, la línea azul coincide perfectamente con la línea verde, es decir, transmiten a la tasa máxima, con lo cual los clientes UDP obtienen el ancho de banda al que transmiten.

Por otro lado, en las gráficas de tráfico TCP, clientes C2 y C4 se aprecia que la línea azul prácticamente coincide con la línea verde, con lo cual se puede decir que los clientes TCP obtienen el ancho de banda al que transmiten. La diferencia con las gráficas de tráfico UDP, es que en las de tráfico TCP se distinguen picos verdes ligeramente por debajo de la línea azul, esto es debido a que se genera tráfico en media y cuando se enfrenta tráfico UDP frente a TCP, el UDP no colabora, es decir, no reduce su ventana de transmisión y continúa transmitiendo a la tasa máxima.

En la tabla de resultados 3.41, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.41: Resultados para fuentes UDP y TCP a 2M "Distintos Contratos" dos colas

Filter ID	Filter- PKTS	Filter-OCTETS	TRAFFIC PROFILE DISCARD PKTS	BW (Mbps)	
UDP					
1 (2,2M)	29254	31418796	0	2,094586	**ORO**
3 (2,6M)	29254	31418796	0	2,094586	**PLATA**
TCP					
4 (1,8M)	25243	31723114	0	2,114874	**ORO**
2 (1,4M)	25350	31730604	0	2,115373	**PLATA**

Todos los clientes obtienen el mismo ancho de banda.
Al **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **2,1M**.

Nota: La ventana de transmisión **no se ajusta perfectamente a 2 Mbps**, ya que el programa *Traffic Generator* transmite en media.

3. Tráfico generado por cada cliente: 3 Mbps

Tráfico total generado: 3 * 4 = 12 Mbps, 120% del ancho de banda total. Por tanto, se forma **cuello de botella en** el enlace final.

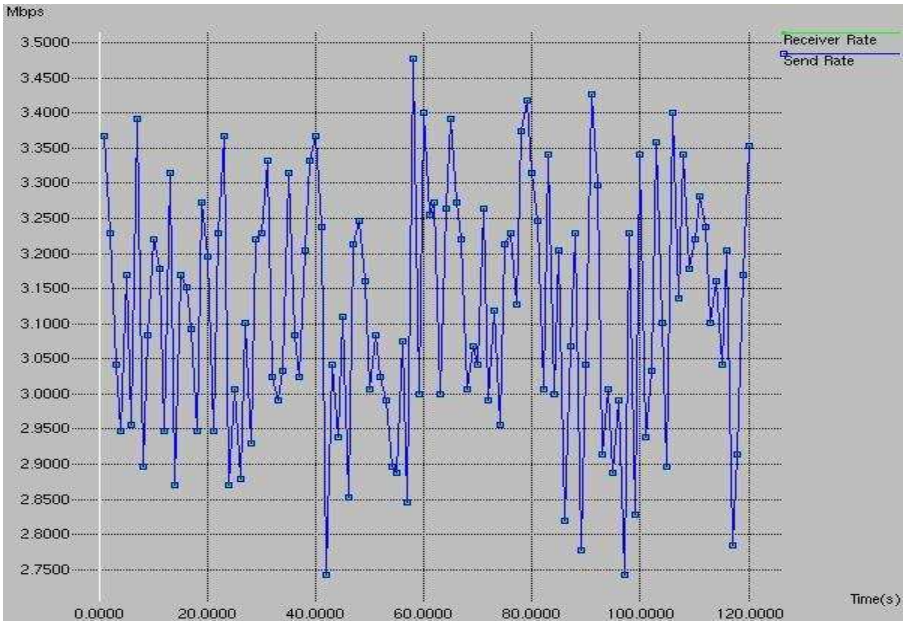


Figura 3.124: C1 (2,2 M) UDP ORO a 3M

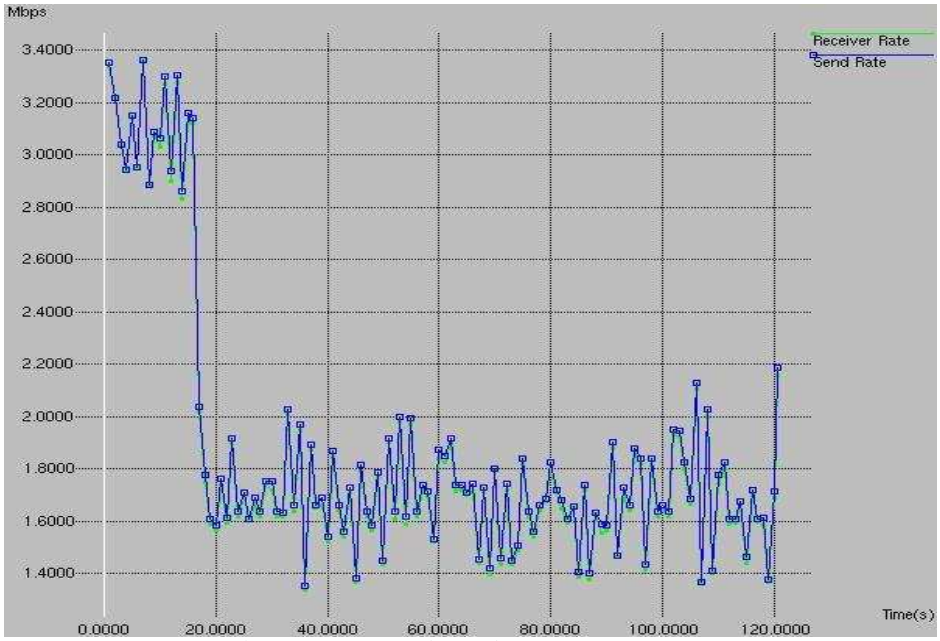


Figura 3.125: C2 (1,4 M) TCP PLATA a 3M

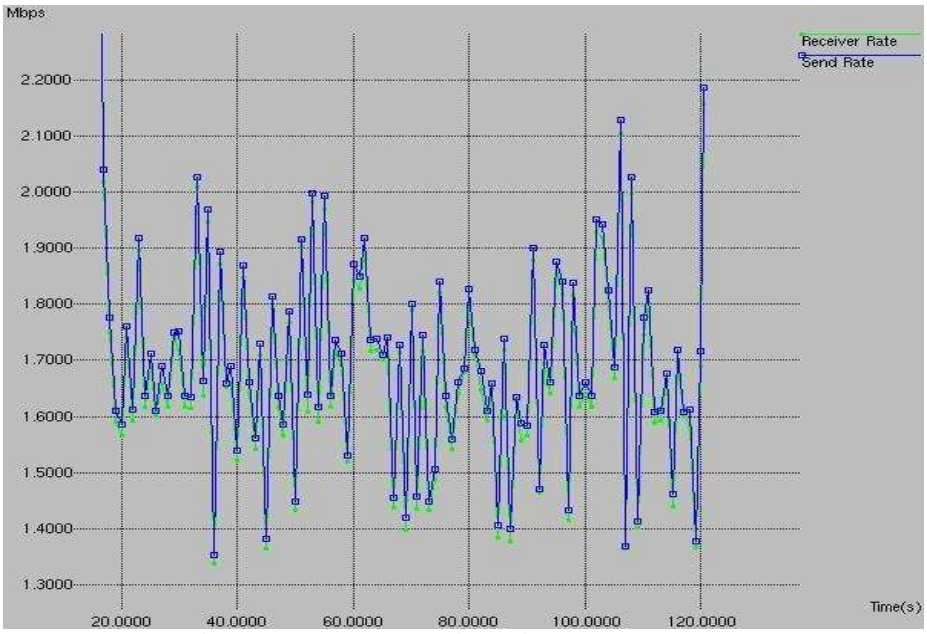


Figura 3.126: Zoom C2 (1,4 M) TCP PLATA a 3M

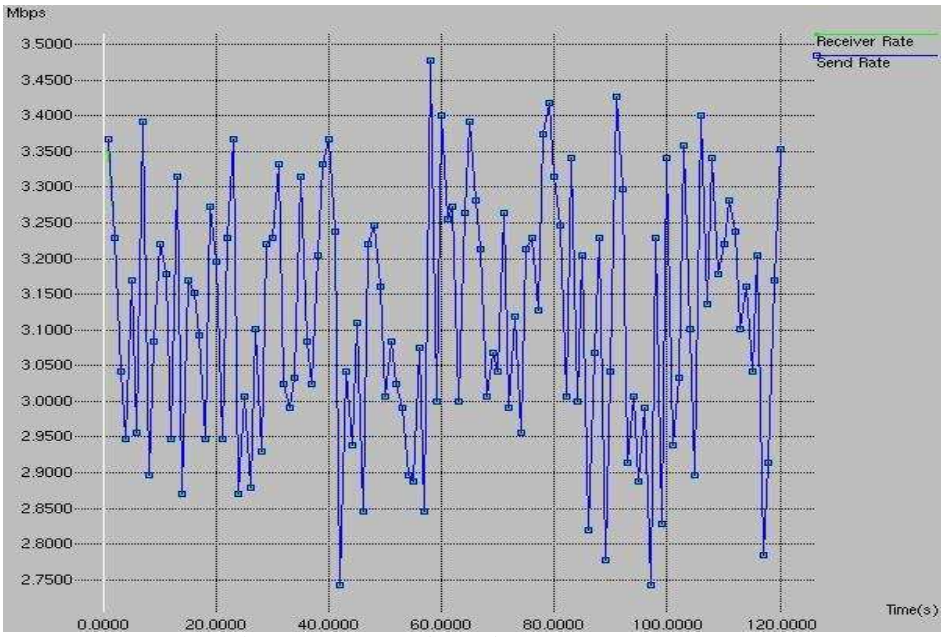


Figura 3.127: C3 (2,6 M) UDP PLATA a 3M

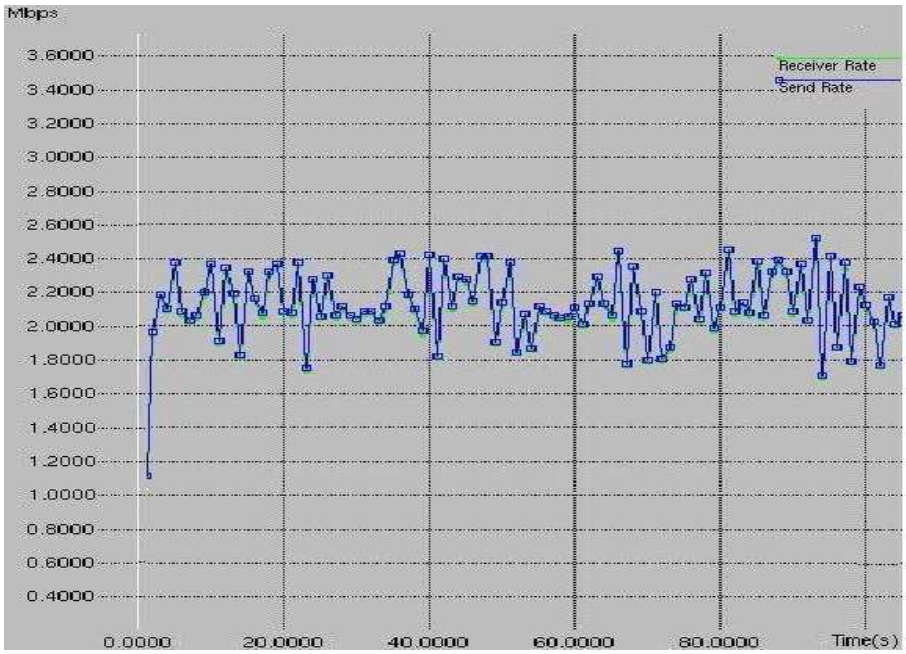


Figura 3.128: C4 (1,8 M) TCP ORO a 3M

En las gráficas de tráfico TCP, clientes C2 y C4, se observa que la línea azul queda ligeramente por encima de la línea verde, ya que en este caso al estar en **situación de congestión** las fuentes TCP no obtienen el ancho de banda máximo al que transmiten.
Los **clientes UDP**, clientes C1 y C3, consiguen los 3M a los que generan tráfico, puesto que las fuentes UDP no se enteran de la congestión y continuarán transmitiendo a la tasa máxima. Del ancho de banda total sobran 2M para cada cliente TCP. En este escenario con dos colas, las fuentes TCP reducen su ventana de transmisión de modo que se reparten el sobrante en función de su **prioridad**. Así, el C2 reduce más su ventana de transmisión que el C4 (el cual tiene mayor prioridad).
Se observa como en un principio el **cliente TCP C2** comienzan a generar tráfico a 3M hasta detectar la congestión, entonces reduce su ventana de transmisión. El **cliente TCP C4**, al empezar a transmitir más tarde, directamente transmite a la ventana de transmisión (2,3M) que le corresponde en esta situación de congestión.

En la tabla de resultados 3.42, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.42: Resultados para fuentes UDP y TCP a 3M "Distintos Contratos" dos colas

Filter ID	Filter- PKTS	Filter-OCTETS	TRAFFIC PROFILE DISCARD PKTS	BW (Mbps)	
UDP					
1 (2,2M)	43796	47036904	0	3,135793	**ORO**
3 (2,6M)	43794	47034756	0	3,135650	**PLATA**
TCP					
4 (1,8M)	23590	35345780	0	2,356385	**ORO**
2 (1,4M)	19897	28617638	0	1,907842	**PLATA**

Al estar en situación de congestión, el tráfico UDP va a conseguir el ancho de banda al que genera tráfico, es decir, los clientes C1 y C3 consiguen un total de aproximadamente 6M del ancho de banda total, quedando alrededor de 4M a repartir entre los clientes C2 y C4.
Al existir dos colas de prioridad, el reparto del ancho de banda (4M) entre los **clientes TCP**, C2 y C4, no es equitativo, sino que depende del peso de cada cola. Así el cliente C4 obtiene mayor ancho de banda (2,35M) pues tiene mayor prioridad de emisión (cola Oro) que el cliente C2 el cual obtiene un ancho de banda de 1,9M (cola Plata).

3.3.3.2.2 Aplicando Servicios Diferenciados (se activa DROP)

- Prueba **contratos C2 y C4 TCP > contratos C1 y C3 UDP**

  En esta prueba, los contratos de las fuentes generadoras de tráfico TCP C2 y C4 son mayores que los contratos de las fuentes generadoras de tráfico UDP C1 y C3.

1. **Tráfico generado por cada cliente: 1,25 Mbps**

   Tráfico total generado: 1,25 * 4 = 5 Mbps, 50% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

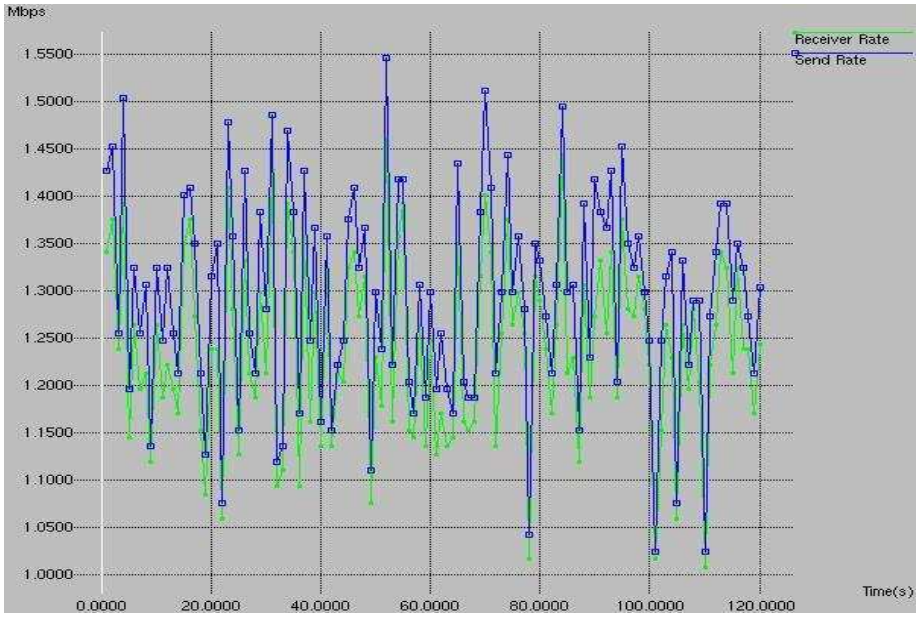


Figura 3.129: C1 (1,4 M) UDP ORO a 1,25M

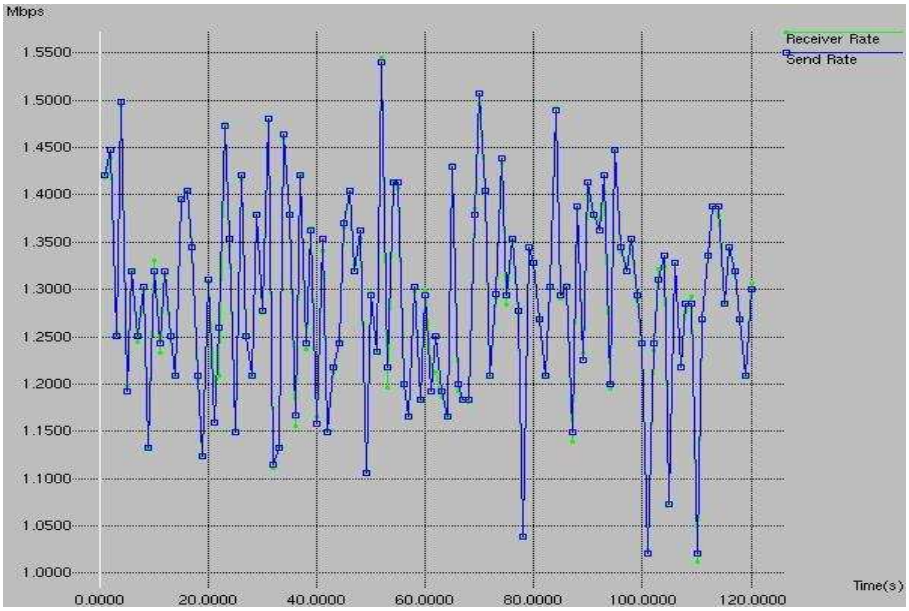


Figura 3.130: C2 (2,2 M) TCP PLATA a 1,25M

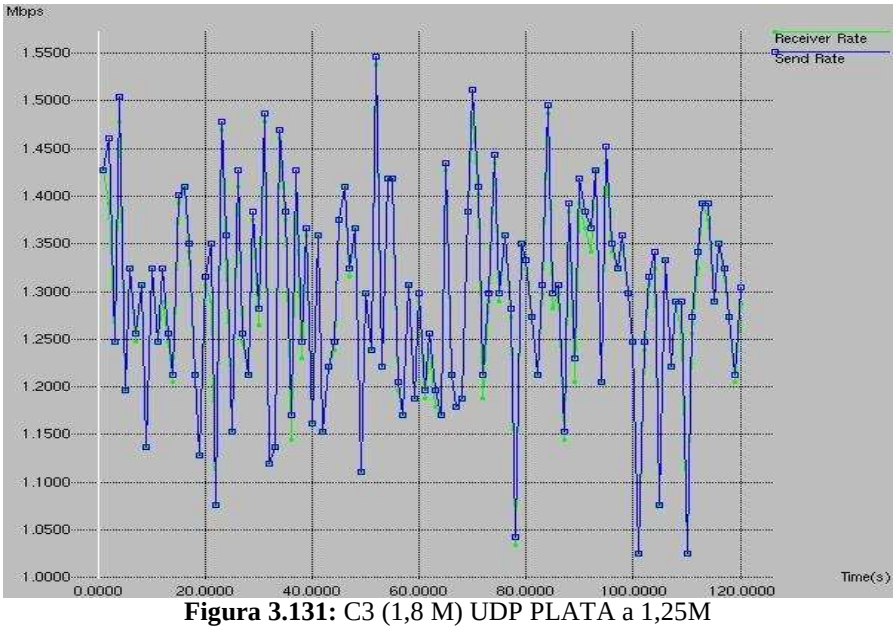


Figura 3.131: C3 (1,8 M) UDP PLATA a 1,25M

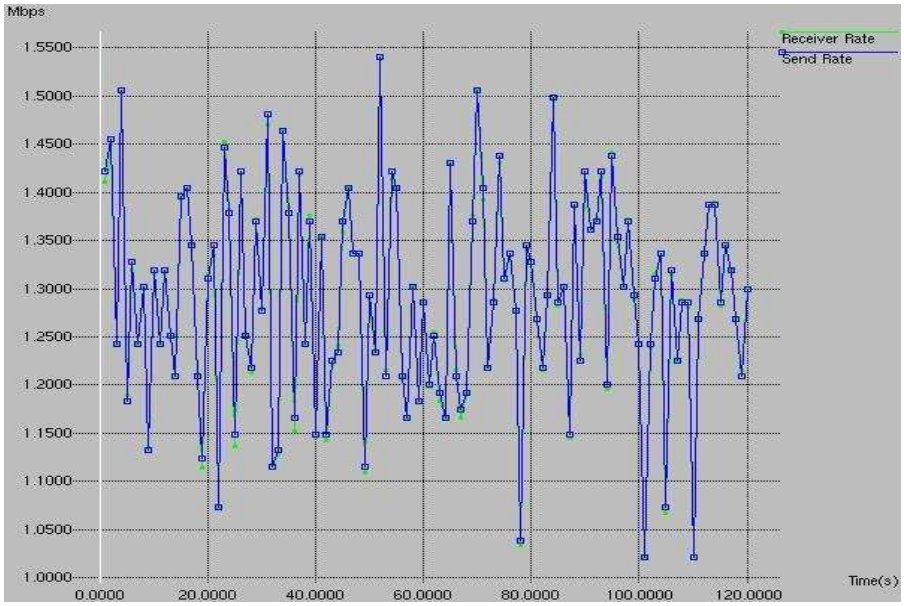


Figura 3.132: C4 (2,6 M) TCP ORO a 1,25M

En las gráficas se observa que conforme disminuye el contrato, mayor es la separación entre la línea azul y línea verde. Así, se deduce que el cliente C1 sufre más descartes de paquetes que el resto de las fuentes porque tiene mayor separación entre dichas líneas, pues es la fuente de menor contrato (1,4M). Aún así, la separación no es significativa pues todos los clientes cumplen su contrato y sobra ancho de banda. El descarte de paquetes se debe a que la transmisión de tráfico es en media.

En la tabla de resultados 3.43, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.43: Resultados para fuentes UDP y TCP a 1,25M "Distintos Contratos" dos colas DROP

Filter ID	Filter-PKTS	Filter-OCTETS	Ventana de transmisión	TRAFFIC PROFILE DISCARD PKTS	BW DESCARTADO	BW (Mbps)	
UDP							
1 (1,4M)	18194	19540356	1,30269	**782**	0,053384	**1,249306**	**ORO**
3 (1,8M)	18194	19540356	1,30269	**114**	0,007782	**1,294908**	**PLATA**
TCP							
4 (2,6M)	17676	19882456	1,325497	**18**	0,001228	**1,324268**	**ORO**
2 (2,2M)	17725	19941462	1,32943	**60**	0,004096	**1,325334**	**PLATA**

Obtiene un mayor ancho de banda las fuentes TCP en torno a 1,32M, en las cuales el contrato es mayor. Aun así, el ancho de banda obtenido es prácticamente el mismo para todas las fuentes en torno a 1,3M, ya que no se está en situación de congestión y todos los clientes cumplen su contrato, por lo que cada cliente se lleva el ancho de banda al que genera tráfico.
El mayor descarte de paquetes se aprecia en el cliente C1 el cual tiene el menor contrato (va a tener más probabilidad de generar mayor número de paquetes que estén fuera del contrato que el resto de clientes), **y es además, fuente UDP**, es decir, transmite a la tasa máxima. Los descartes de

paquetes no son significativos, ya que es por generar tráfico en media, y no porque falte ancho de banda.

Nota: La ventana de transmisión **no se ajusta perfectamente a 1,25 Mbps**, ya que el programa *Traffic Generator* transmite en media.

2. Tráfico generado por cada cliente: 2 Mbps

Tráfico total generado: 2 * 4 = 8 Mbps, 80% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

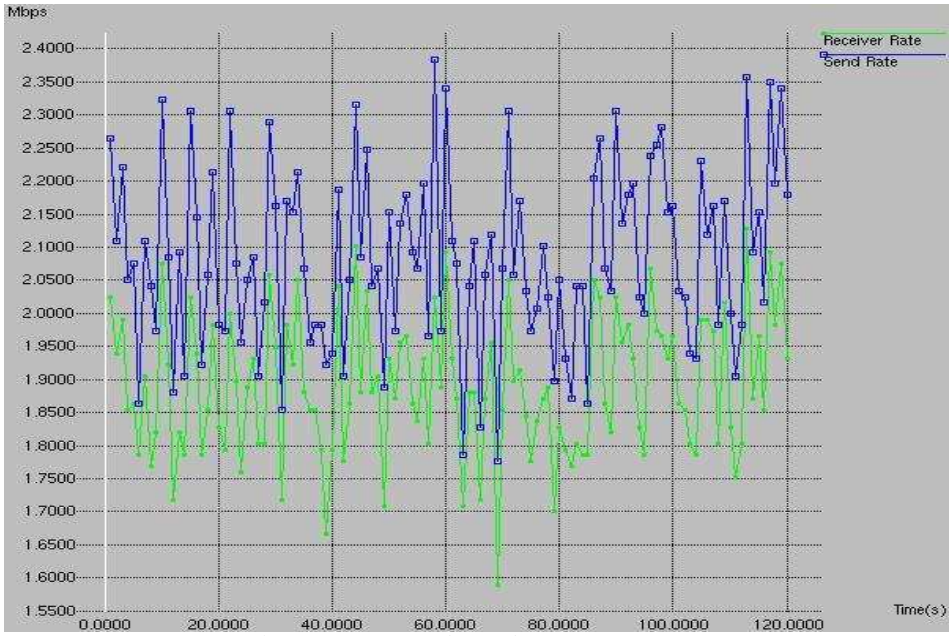


Figura 3.133: C1 (1,4 M) UDP ORO a 2M

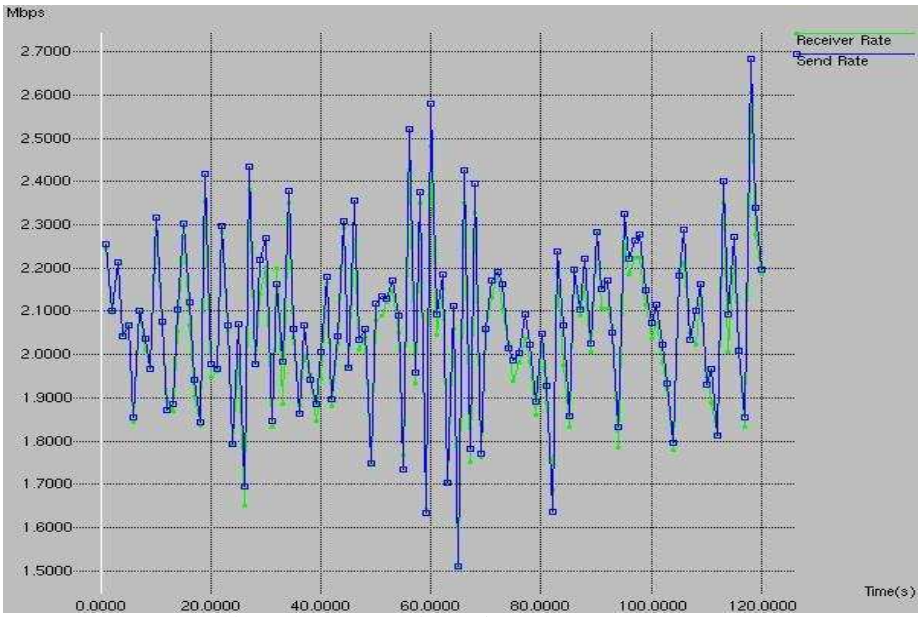


Figura 3.134: C2 (2,2 M) TCP PLATA a 2M

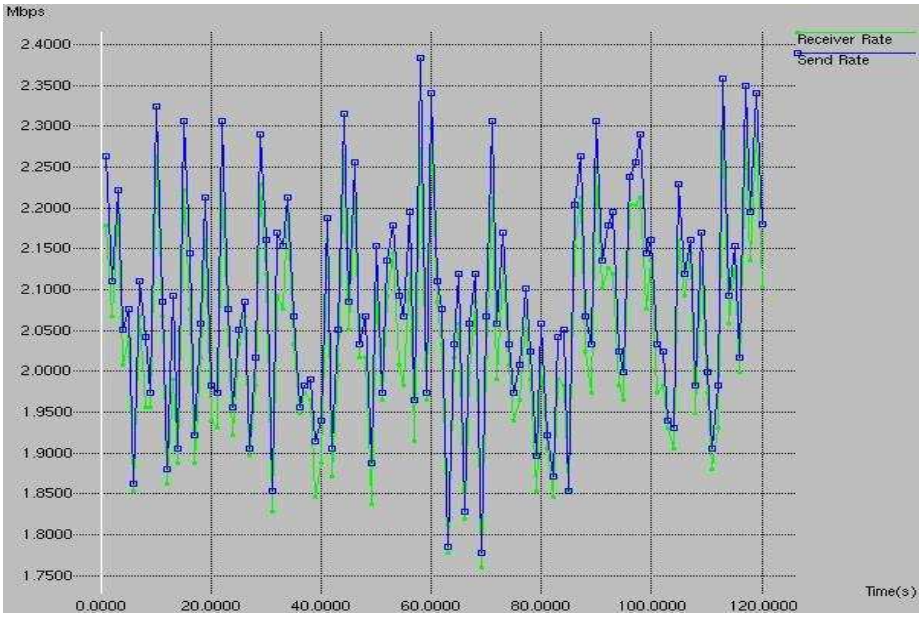


Figura 3.135: C3 (1,8 M) UDP PLATA a 2M

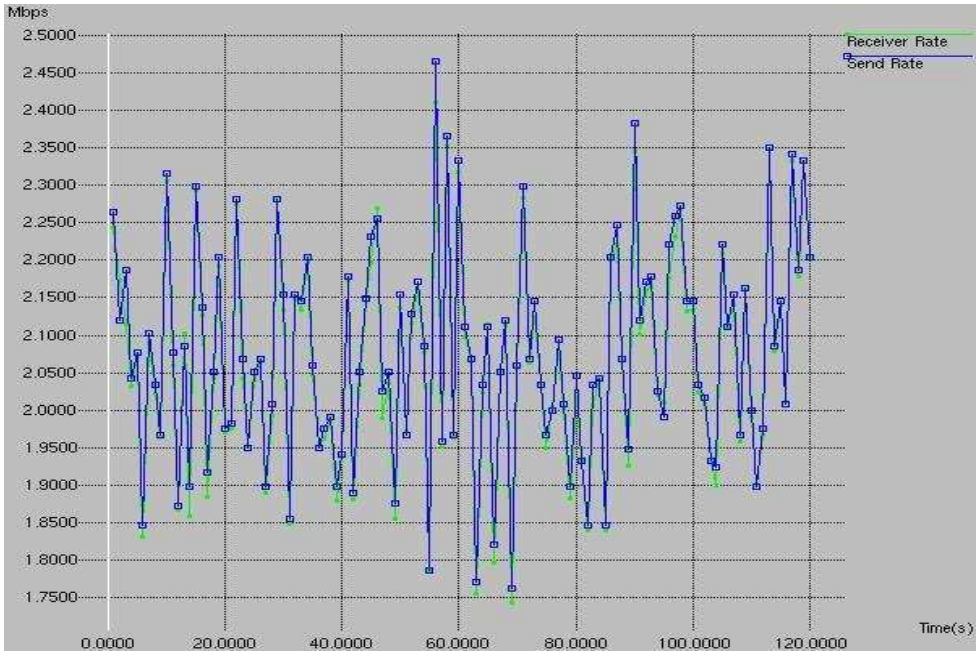


Figura 3.136: C4 (2,6 M) TCP ORO a 2M

En este escenario se ocupa el 80% del canal, con lo cual se está en el límite a partir del cual las prestaciones de la red comienzan a degradarse. Pasado este límite el tráfico UDP acapara los recursos frente al tráfico TCP.

Al aplicar Servicios Diferenciados, se observa que en las gráficas de tráfico UDP, clientes C1 y C3, la línea azul y la verde se separan ligeramente. Esto es debido a los descartes que sufre. La separación es mayor en el cliente C1 por tener menor contrato. Aún así, se obtiene el ancho de banda al que transmite, ya que **hay ancho de banda de sobra** para todas las fuentes.

Por otro lado, en las gráficas de tráfico TCP, clientes C2 y C4 se aprecia que la línea azul prácticamente coincide con la línea verde, con lo cual los clientes TCP obtienen el ancho de banda al que transmiten.

En la tabla de resultados 3.44, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.44: Resultados para fuentes UDP y TCP a 2M "Distintos Contratos" dos colas DROP

Filter ID	Filter-PKTS	Filter-OCTETS		TRAFFIC PROFILE DISCARD PKTS	BW DESCARTADO	BW (Mbps)	
UDP							
1 (1,4M)	29252	31416648	2,094443	**2711**	0,217603	**1,87684**	**ORO**
3 (1,8M)	29252	31416648	2,094443	**602**	0,041096	**2,05334**	**PLATA**
TCP							
4 (2,6M)	26360	32037912	2,135861	**219**	0,01495	**2,12091**	**ORO**
2 (2,2M)	25393	33531718	2,235448	**1390**	0,094891	**2,14055**	**PLATA**

Al **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **2M** ya que el programa generador de tráfico *Traffic Generator* genera en media.

En las fuentes TCP, se observa que el cliente C4 por tener el mayor contrato y mayor prioridad sufre menor descarte de paquetes. El cliente TCP C2 a pesar de tener mayor contrato que el cliente UDP C3 sufre más descartes **debido al propio descarte**, ya que TCP detecta las pérdidas y **reenvía los paquetes descartados**. El mayor descarte de paquetes se aprecia en el C1 el cual tiene el menor contrato y **es además fuente UDP**, es decir, todo el tiempo transmite a la tasa máxima.

Nota: La ventana de transmisión **no se ajusta perfectamente a 2 Mbps**, ya que el programa *Traffic Generator* transmite en media.

3. **Tráfico generado por cada cliente: 3 Mbps**

   Tráfico total generado: 3 * 4 = 12 Mbps, 120% del ancho de banda total. Por tanto, se forma **cuello de botella en** el enlace final.

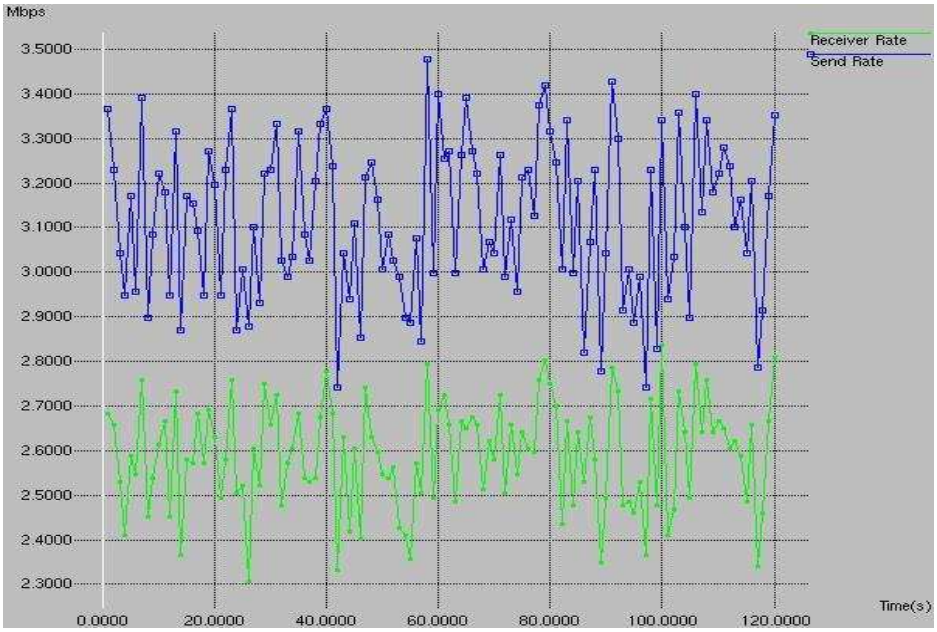


Figura 3.137: C1 (1,4 M) UDP ORO a 3M

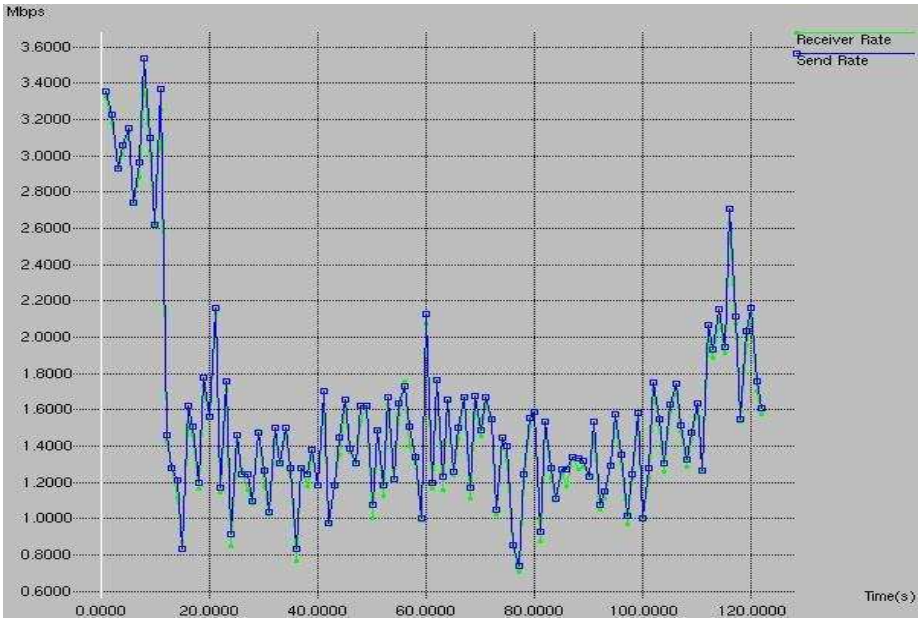


Figura 3.138: C2 (2,2 M) TCP PLATA a 3M

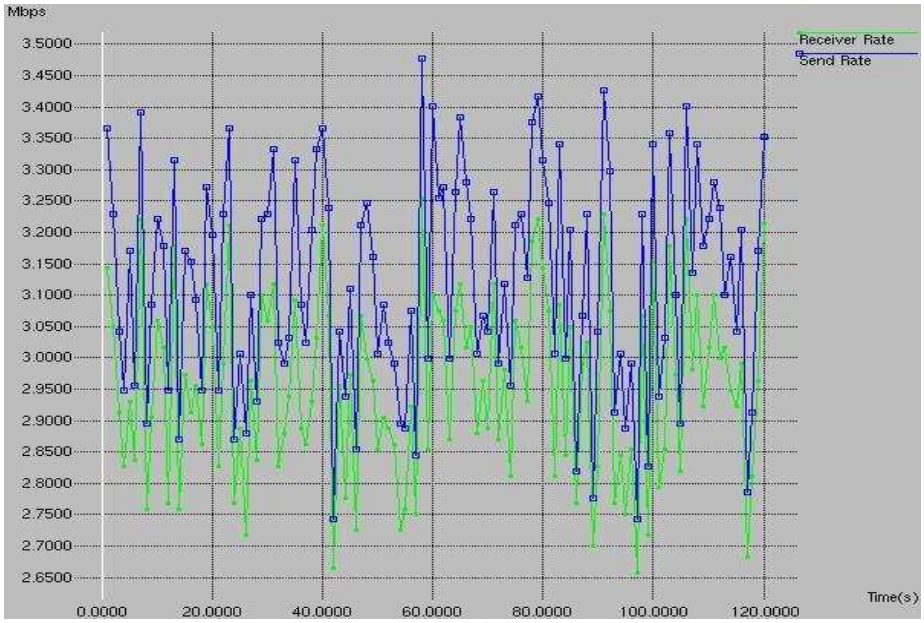


Figura 3.139: C3 (1,8 M) UDP PLATA a 3M

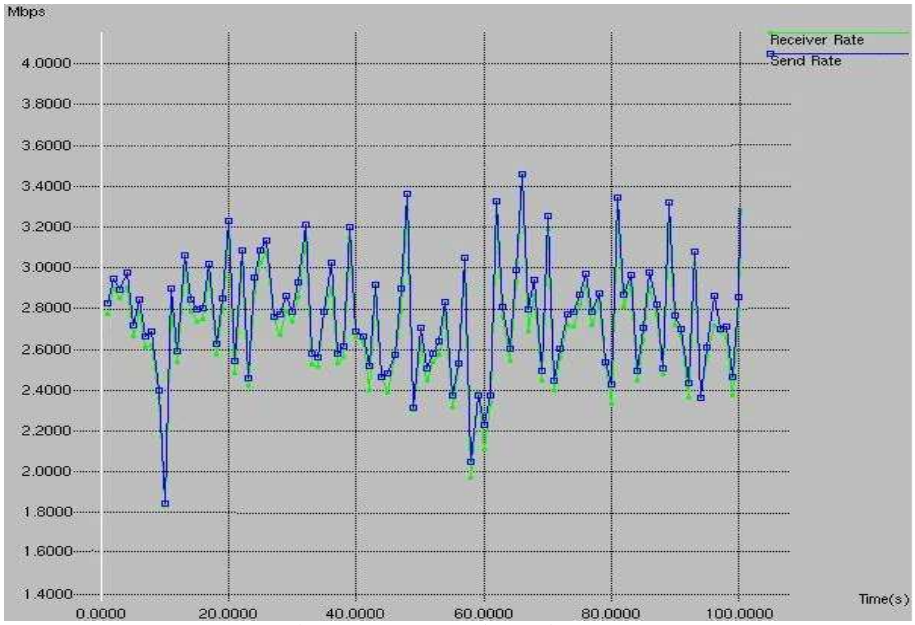


Figura 3.140: C4 (2,6 M) TCP ORO a 3M

En este caso, todas las fuentes comienzan transmitiendo a 3M y por tanto se produce congestión.
En las gráficas se observa que los clientes con menor contrato no obtienen el menor ancho de banda como cabría esperar. Así, el cliente C1, el de menor contrato (1,4M), obtiene en torno a 2,6M; y el cliente C3, de contrato (1,8M), obtiene prácticamente los 3M a los que transmite. Esto se debe a que en este escenario **se enfrenta tráfico TCP con tráfico UDP**. Las fuentes UDP no se enteran de la congestión por lo que **no reducen su ventana de transmisión**, por lo que intentan transmitir a 3M todo el tiempo, es decir, acaparar todos los recursos.

Al **aplicar Servicios Diferenciados**, la fuente UDP con menor contrato C1 sufre una disminución de 0,5M respecto al ancho de banda al que transmite, y la fuente TCP C2 detecta la congestión y reduce bruscamente su ventana de transmisión de 3M a unos **1,7M**. Gracias a esta reducción y al descarte de paquetes en la fuente UDP C1, el cliente TCP C4 puede mantener su ventana de transmisión y obtener los 3M a los que transmite tráfico. El cliente C4 es el que tiene mayor contrato 2,6M (valor cercano a los 3M a los que las fuentes generan tráfico) y mayor prioridad (cola Oro).
En las gráficas el descarte de paquetes se traduce en la separación entre la línea azul y la línea verde, cuanto mayor es la separación mayor es el descarte. En la gráfica del cliente UDP C1 al tener el menor contrato y por ser fuente UDP se aprecia la mayor separación entre la línea azul y la línea verde, esto es, es el que sufre mayor descarte de paquetes (no se reenvían como ocurre con el tráfico TCP).
Comparando con las gráficas cuando **no se aplican servicios diferenciados**, ahora se tienen en cuenta **los contratos**, **el tipo de tráfico** UDP o TCP y el peso de cola (plata u oro) para el reparto del ancho de banda no contratado.

En la tabla de resultados 3.45, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.45: Resultados para fuentes UDP y TCP a 3M "Distintos Contratos" dos colas DROP

Filter ID	Filter-PKTS	Filter-OCTETS	Ventana de transmisión	TRAFFIC PROFILE DISCARD PKTS	BW DESCARTADO	BW (Mbps)	
UDP							
1 (1,4M)	43794	47034756	3,13565	**6648**	0,475993	**2,659657**	**ORO**
3 (1,8M)	43794	47034756	3,13565	**2605**	0,186535	**2,949115**	**PLATA**
TCP							
4 (2,6M)	33546	50843124	3,389542	**2551**	0,174148	**3,173868**	**ORO**
2 (2,2M)	18161	26938550	1,795903	**2032**	0,200968	**1,594935**	**PLATA**

Ahora se está en situación de congestión y cada cliente obtiene un ancho de banda distinto en función de su contrato, el tipo de tráfico UDP o TCP y la cola a la que es asignado.

El **descarte** de paquetes depende del contrato de cada cliente, de su ventana de transmisión, del tipo de tráfico que se transmita UDP o TCP y de la clase de servicio a la que son asignados. Es mayor cuanto menor sea el contrato de los clientes. En el caso del cliente TCP C4, se da un numeroso descarte de paquetes debido a que la cola oro se desborda y el tráfico TCP se ve afectado a pesar de tener mayor contrato (2,6M) frente a UDP tirando en proporción mayor número de paquetes.

Obtiene un **mayor ancho de banda las fuentes UDP** ya que éstas no reducen su ventana de transmisión pero se descartan mayor número de paquetes que en las fuentes TCP, por tener menor contrato y no reducir su ventana de transmisión. El cliente UDP C1 cuyo contrato es el menor, obtiene **2,6M** perdiendo un ancho de banda de 0,47M. El cliente UDP C3 consigue prácticamente los 3M a los que transmite.
El cliente TCP C2 reduce drásticamente su ventana de transmisión por pertenecer a la cola plata que es de menor prioridad, logrando sólo **1,59M** del ancho de banda total del enlace final, y así el cliente TCP C4 puede mantener su ventana de transmisión (3M). También se observa cómo la **cola oro** tiene **mayor más prioridad** que la plata y se lleva la mayor parte del ancho de banda. Además, el cliente C4 logra conservar el ancho de banda al que transmite tráfico 3M acosta del descarte de paquetes del cliente UDP C1.

INTERCAMBIO DE CONTRATOS

- Prueba **contratos C2 y C4 TCP < contratos C1 y C3 UDP**

  En esta prueba, los contratos de las fuentes generadoras de tráfico TCP C2 y C4 son **menores** que los contratos de las fuentes generadoras de tráfico UDP C1 y C3.

1. **Tráfico generado por cada cliente: 1,25 Mbps**

   Tráfico total generado: 1,25 * 4 = 5 Mbps, 50% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

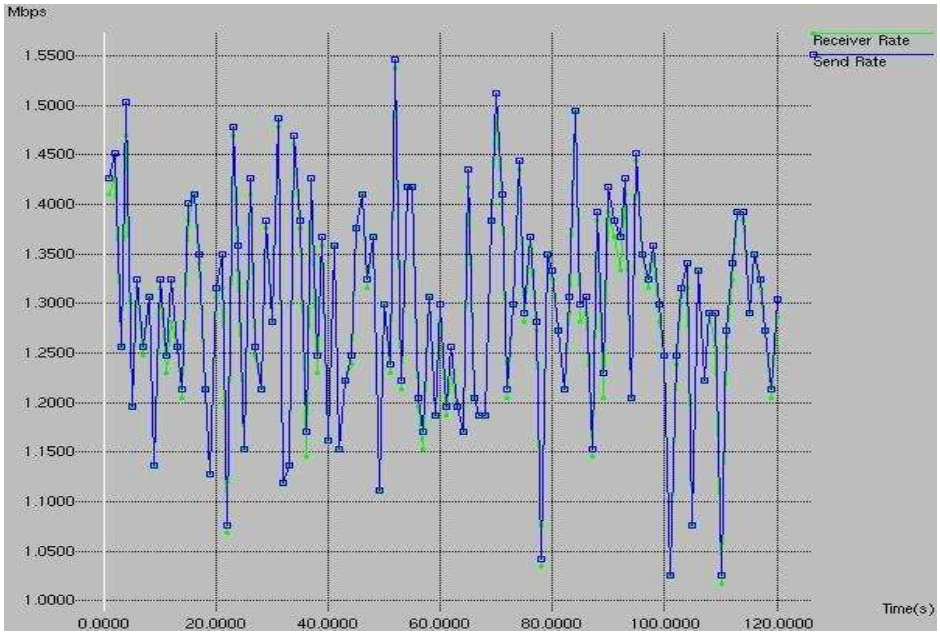


Figura 3.141: C1 (2,2 M) UDP ORO a 1,25M

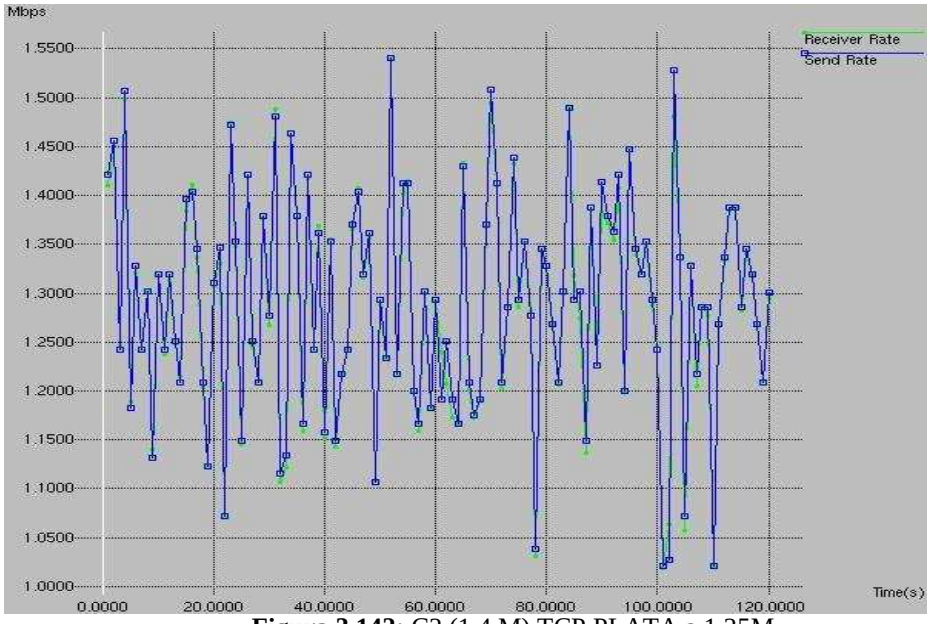


Figura 3.142: C2 (1,4 M) TCP PLATA a 1,25M

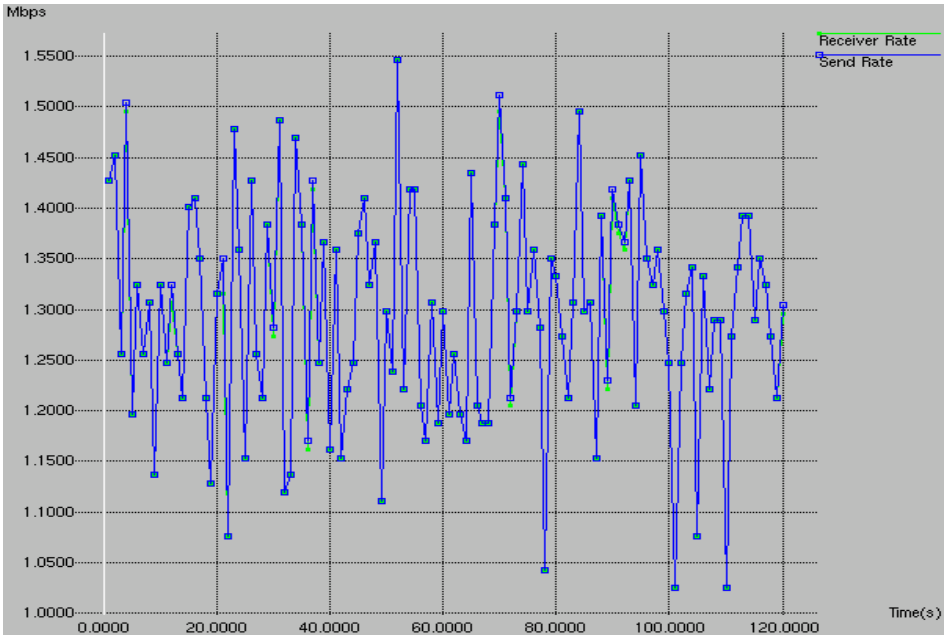


Figura 3.143: C3 (2,6 M) UDP PLATA a 1,25M

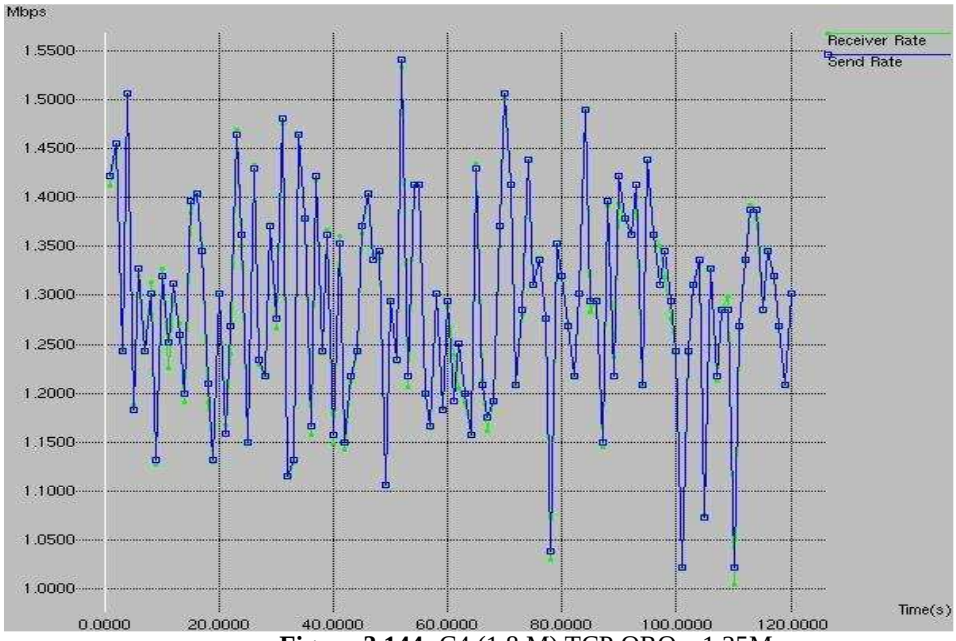


Figura 3.144: C4 (1,8 M) TCP ORO a 1,25M

Todos los clientes cumplen su contrato y sobra ancho de banda. El descarte de paquetes se debe a que la transmisión de tráfico es en media.
El ancho de banda obtenido es prácticamente el mismo para todas las fuentes en torno a 1,3M, ya que no se está en situación de congestión y todos los clientes cumplen su contrato, por lo que cada cliente se lleva el ancho de banda al que genera tráfico.
Los descartes de paquetes no son significativos, ya que es por generar tráfico en media, y no porque falte ancho de banda.

Nota: La ventana de transmisión **no se ajusta perfectamente a 1,25 Mbps**, ya que el programa *Traffic Generator* transmite en media.

En la tabla de resultados 3.46, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.46: Resultados para fuentes UDP y TCP a 1,25M "Distintos Contratos" dos colas DROP

Filter ID	Filter-PKTS	Filter-OCTETS	Ventana de transmisión	TRAFFIC PROFILE DISCARD PKTS	BW DESCARTADO	BW (Mbps)	
UDP							
1 (2,2M)	18194	19540356	1,30269	**120**	0,008192	**1,294498**	**ORO**
3 (2,6M)	18194	19540356	1,30269	**18**	0,001228	**1,301461**	**PLATA**
TCP							
4 (1,8M)	17754	20003348	1,333556	**117**	0,007987	**1,325569**	**ORO**
2 (1,4M)	17760	20053688	1,336912	**152**	0,010376	**1,326536**	**PLATA**

El descarte de paquetes de C1 ahora es menor ya que ha aumentado su contrato de 1,4M a 2,2M. Lo mismo sucede con C3. Por el contrario se observa como los clientes C2 y C4 ven aumentado su número de paquetes descartados debido a la reducción en sus contratos.

2. Tráfico generado por cada cliente: 2 Mbps

Tráfico total generado: 2 * 4 = 8 Mbps, 80% del ancho de banda total. Por tanto, no se forma cuello de botella en el enlace final.

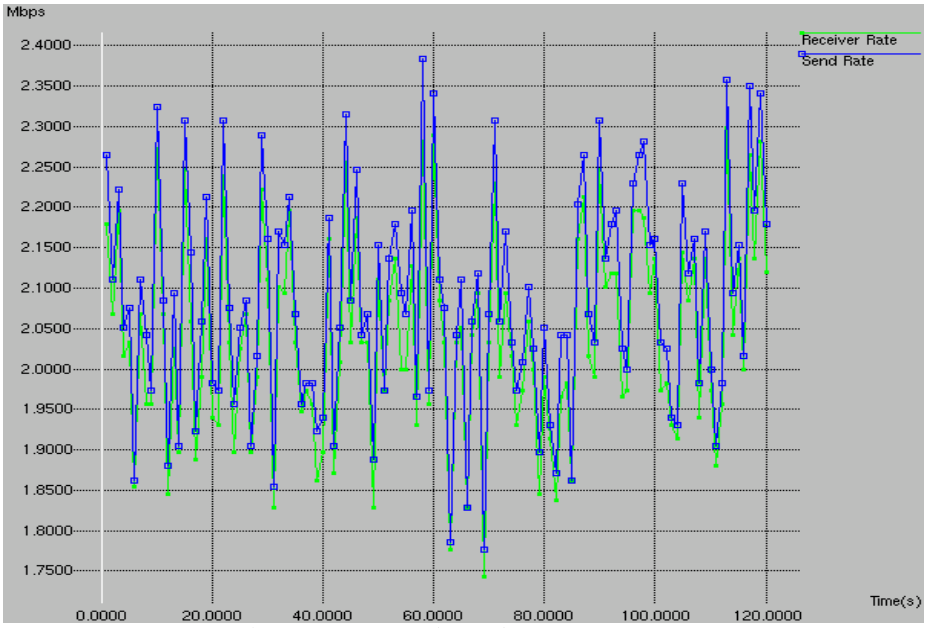


Figura 3.145: C1 (2,2 M) UDP ORO a 2M

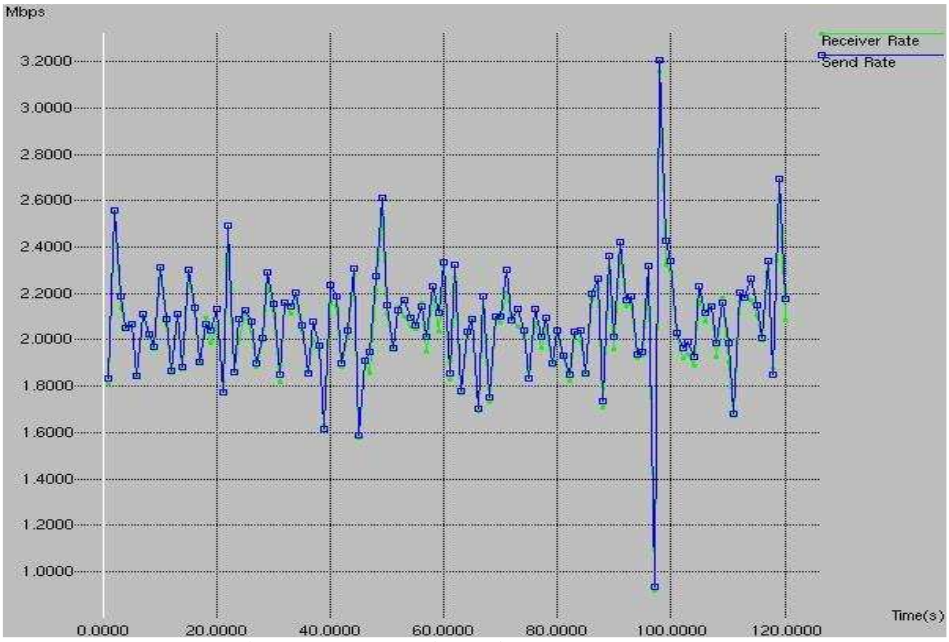


Figura 3.146: C2 (1,4 M) TCP PLATA a 2M

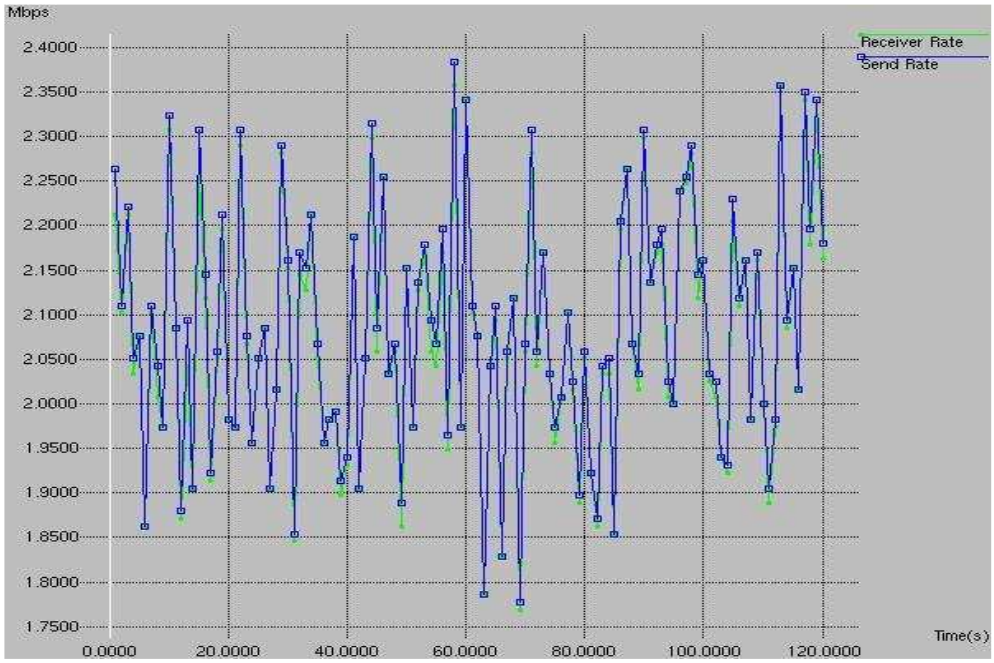


Figura 3.147: C3 (2,6 M) UDP PLATA a 2M

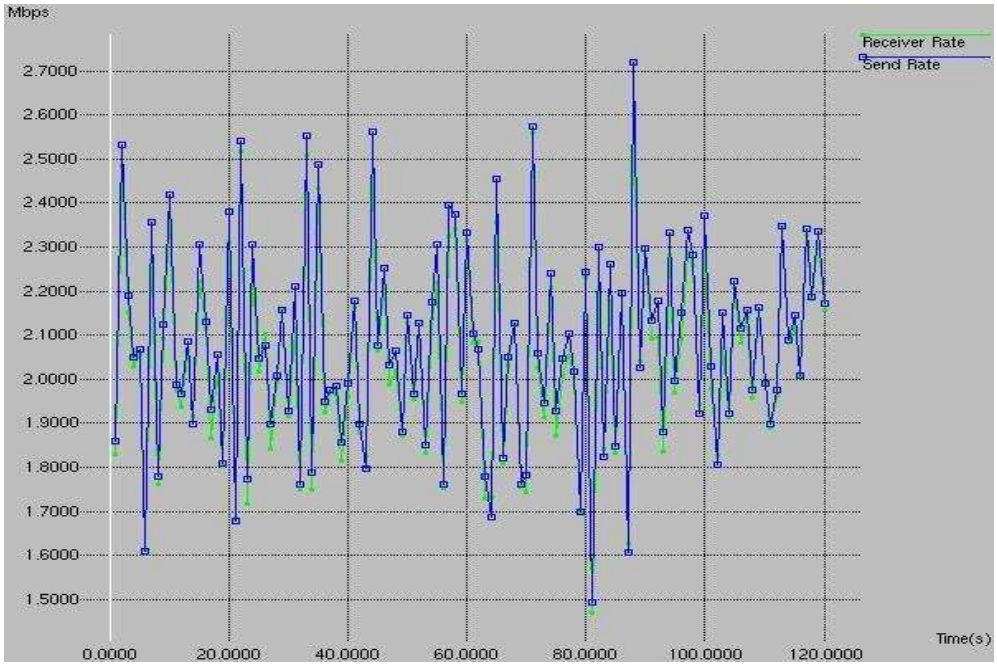


Figura 3.148: C4 (1,8 M) TCP ORO a 2M

En este escenario se ocupa el 80% del canal, con lo cual se está en el límite a partir del cual las prestaciones de la red comienzan a degradarse. Pasado este límite el tráfico UDP acapara los recursos frente al tráfico TCP.
Al aplicar Servicios Diferenciados, se observa que en las gráficas la línea azul y la verde se separan ligeramente. Esto es debido a los descartes que sufren los clientes.
Se obtiene el ancho de banda al que transmiten, ya que **hay ancho de banda de sobra** para todas las fuentes.

En la tabla de resultados 3.47, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.47: Resultados para fuentes UDP y TCP a 2M "Distintos Contratos" dos colas DROP

Filter ID	Filter-PKTS	Filter-OCTETS	Ventana de transmisión	TRAFFIC PROFILE DISCARD PKTS	BW DESCARTADO	BW (Mbps)	
UDP							
1 (2,2M)	29252	31416648	2,094443	**604**	0,041233	**2,0532**	**ORO**
3 (2,6M)	29252	31416648	2,094443	**132**	0,009011	**2,08543**	**PLATA**
TCP							
4 (1,8M)	25740	33515656	2,234377	**1386**	0,094617	**2,139759**	**ORO**
2 (1,4M)	25595	33645058	2,243003	**1457**	0,099464	**2,143539**	**PLATA**

En este escenario, el tráfico UDP tiene mayor contrato, por ello el C1 consigue ver aumentado su ancho de banda conseguido de 1,87M a 2,05M.
Al **no estar en situación de congestión** cada cliente se lleva el ancho de banda al que genera tráfico, en torno a **2M** ya que el programa generador de tráfico *Traffic Generator* genera en media.

En las fuentes UDP, se observa que el cliente C3 por tener el mayor contrato sufre el menor descarte de paquetes. El mayor descarte de paquetes se aprecia en el cliente TCP C2 el cual tiene el menor contrato.

Nota: La ventana de transmisión **no se ajusta perfectamente a 2 Mbps**, ya que el programa *Traffic Generator* transmite en media.

3. Tráfico generado por cada cliente: 3 Mbps

Tráfico total generado: 3 * 4 = 12 Mbps, 120% del ancho de banda total. Por tanto, se forma **cuello de botella en** el enlace final.

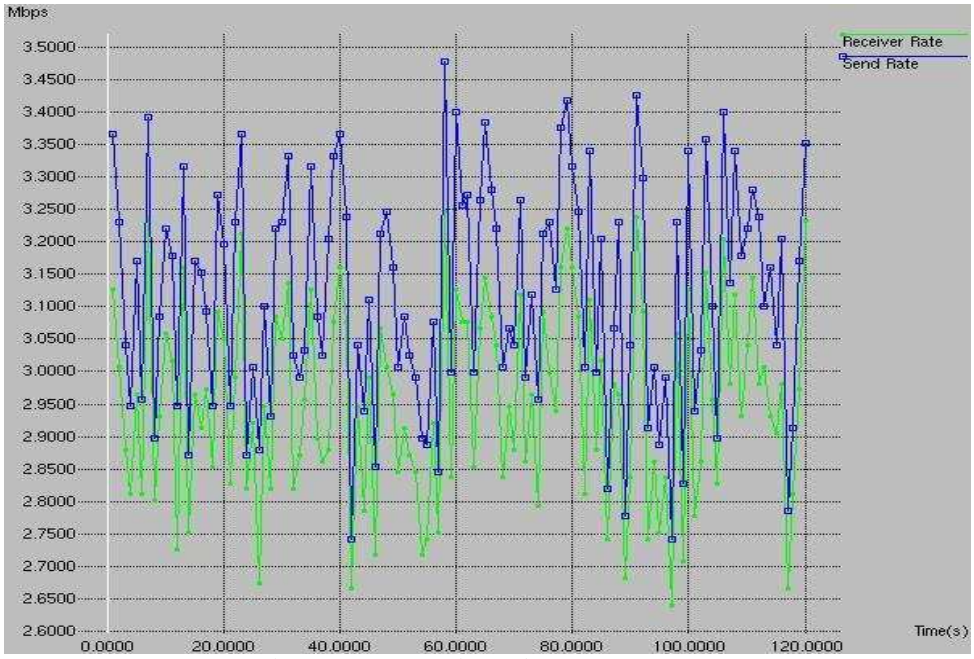


Figura 3.149: C1 (2,2 M) UDP ORO a 3M

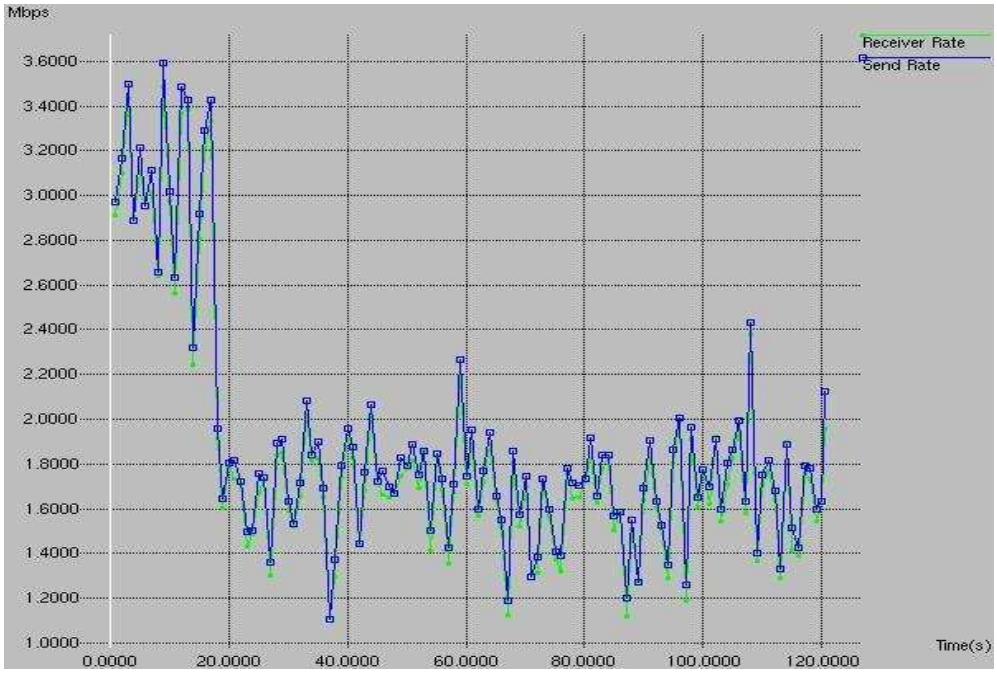


Figura 3.150: C2 (1,4 M) TCP PLATA a 3M

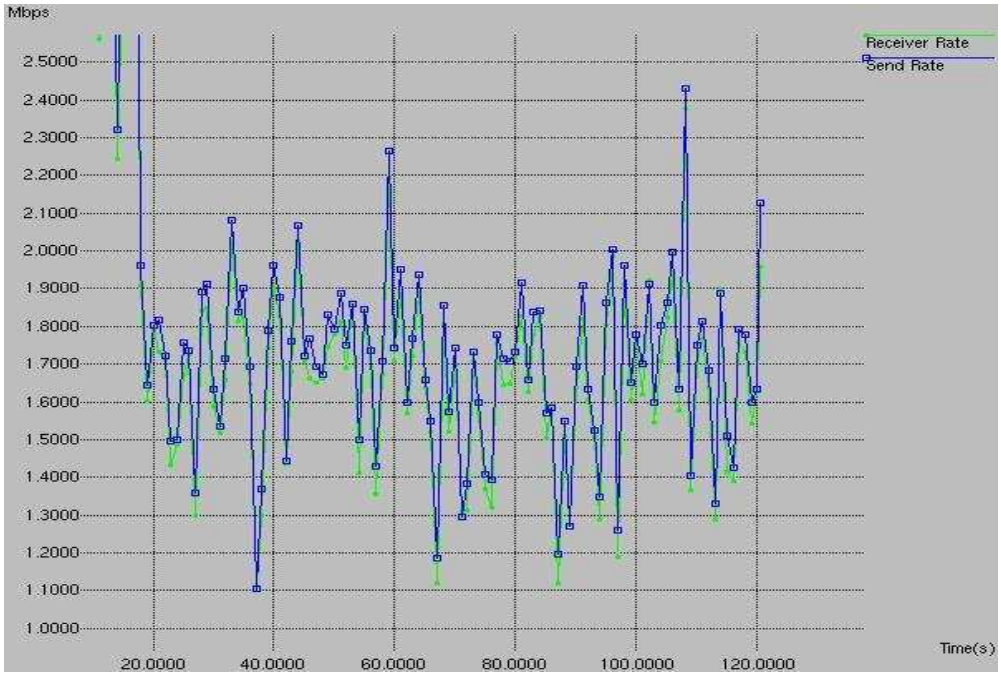


Figura 3.151: Zoom C2 (1,4 M) TCP PLATA a 3M

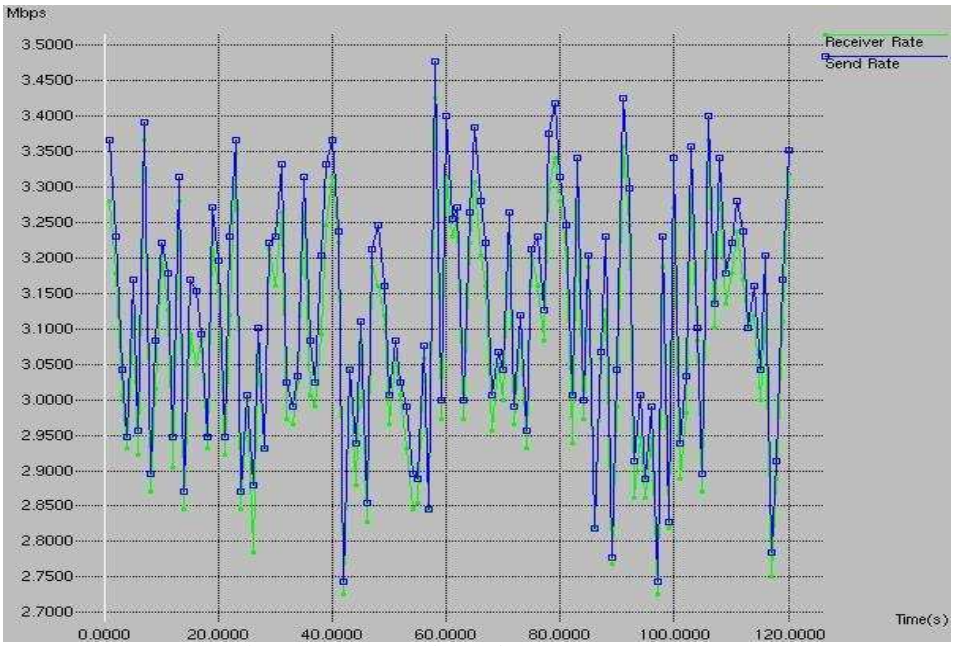


Figura 3.152: C3 (2,6 M) UDP PLATA a 3M

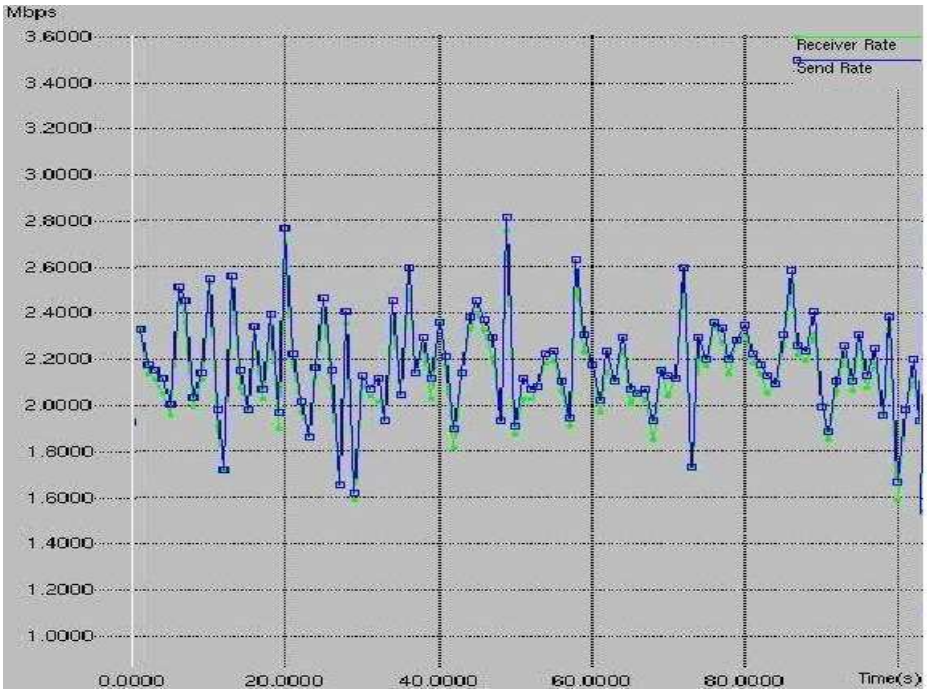


Figura 3.153: C4 (1,8 M) TCP ORO a 3M

En este caso, todas las fuentes comienzan transmitiendo a 3M y por tanto se produce congestión.
En las gráficas se observa que los clientes con menor contrato obtienen el menor ancho de banda. Así, el cliente TCP C2, el de menor contrato (1,4M), obtiene en torno a 2M; y el cliente TCP C4, de contrato (1,8M), obtiene en torno a 2,4M.

Al **aplicar Servicios Diferenciados**, la fuente UDP con menor contrato C1 (2,2M) sufre una disminución de 0,16M respecto al ancho de banda al que transmite, y la fuente TCP C2 detecta la congestión y reduce bruscamente su ventana de transmisión de 3M a unos **2,1M**. El cliente TCP C4 reduce menos su ventana de transmisión 3M a unos **2,6M**. Las fuentes TCP no consiguen los 3M a los que transmiten porque tienen menor contrato que el tráfico UDP.

En las gráficas el descarte de paquetes se traduce en la separación entre la línea azul y la línea verde, cuanto mayor es la separación mayor es el descarte. En la gráfica del cliente UDP C1 al tener menor contrato que la fuente UDP C3 se aprecia la mayor separación entre la línea azul y la línea verde, esto es, sufre mayor descarte de paquetes. La fuente UDP C3 apenas presenta separación pues es la que tiene mayor contrato obteniendo los 3M a los que transmite.

Comparando con las gráficas cuando **no se aplican servicios diferenciados**, ahora se tienen en cuenta **los contratos**, **el tipo de tráfico** UDP o TCP y el peso de cola (Plata u Oro) para el reparto del ancho de banda no contratado.

En la tabla de resultados 3.48, se observan los valores numéricos del ancho de banda obtenido por cada cliente.

Tabla 3.48: Resultados para fuentes UDP y TCP a 3M "Distintos Contratos" dos colas DROP

Filter ID	Filter-PKTS	Filter-OCTETS	Ventana de transmission	TRAFFIC PROFILE DISCARD PKTS	BW DESCARTADO	BW (Mbps)	
UDP							
1 (2,2M)	43794	47034756	3,13565	**2332**	0,159197	**2,629657**	**ORO**
3 (2,6M)	43794	47034756	3,13565	**587**	0,040072	**3,095578**	**PLATA**
TCP							
4 (1,8M)	25700	39006424	2,600428	**2564**	0,175035	**2,425392**	**ORO**
2 (1,4M)	21416	31789560	2,119304	**2101**	0,143428	**1,975875**	**PLATA**

Ahora se está en situación de congestión y cada cliente obtiene un ancho de banda distinto en función de su contrato, el tipo de tráfico UDP o TCP y la cola a la que es asignado.

El **descarte** de paquetes depende del contrato de cada cliente, de su ventana de transmisión, del tipo de tráfico que se transmita UDP o TCP y de la clase de servicio a la que son asignados. Es mayor cuanto menor sea el contrato de los clientes.
Obtiene un **mayor ancho de banda las fuentes UDP**, ya que éstas, tienen mayor contrato que las fuentes TCP.
Además, el cliente C3 logra conservar el ancho de banda al que transmite tráfico 3M acosta del descarte de paquetes del cliente UDP C1 por tener menor contrato.

Capítulo 4

Conclusiones

Hoy en día, debido al crecimiento exponencial del número de usuarios en Internet y al desarrollo emergente de nuevos servicios que generan distintos tipos de tráfico que requieren mayor número de recursos para conseguir unos niveles de funcionamiento adecuados, es necesario dotar de **inteligencia** a las redes de datos mediante la implementación de QoS para gestionar eficientemente el reparto del ancho de banda disponible. En este proyecto se han empleado las herramientas de QoS que el equipo Nortel *Passport 8600 Routing Switch* aplica. Nortel emplea el modelo de arquitectura de Servicios Diferenciados.

Se ha comprobado el funcionamiento del *router Passport 8600 Routing Switch* en un entorno de Servicios Diferenciados empleando los **mecanismos de encolamiento WRR**, con la intención de ver si los proveedores de servicios de Internet podían **garantizar contratos** y conseguir al mismo tiempo **repartir el ancho de banda** de la manera más justa posible. Para ello se llevaron a cabo una serie de experimentos sobre una topología de red en la que se creaba un cuello de botella en el enlace final que unía la interfaz de salida con el servidor y se generaba tráfico desde tres redes LAN. Usando diferentes configuraciones de Servicios Diferenciados se obtuvieron resultados sobre cómo era tratado ese tráfico. Lo primero que se hacía en todas esas pruebas era **medir** el tráfico a la entrada y **marcarlo** aplicando las **políticas de QoS** correspondientes a cada flujo generado por su respectivo cliente. Si el tráfico estaba dentro del contrato se marcaba con un DSCP y si lo sobrepasaba se marcaba con otro.
Se obtuvieron resultados para **dos grupos de pruebas**: configuraciones sin ningún tipo de diferenciación de servicios y configuraciones con diferenciación de servicios. A su vez, estos dos grupos de pruebas se experimentaron en **dos escenarios generales**: caso con una cola (Plata) y caso con dos colas (Plata y Oro). Además, se han llevado a cabo pruebas con diferentes tipos de tráfico TCP y UDP, y con el mismo contrato configurado para todos los clientes o con distinto contrato para cada cliente, para ver cómo reaccionaba el *router* ante diversas situaciones.
Para el primer grupo de pruebas, no se descartaban paquetes por lo que todos los paquetes se trataban por igual independientemente de cómo estuvieran marcados, es decir, independientemente de si pertenecían a una red LAN o a otra o si cumplían o no los contratos. Para el caso con dos colas el tráfico es tratado con independencia de sus contratos pero sí depende de la prioridad de la cola a la que es asignado.
Para el segundo grupo de pruebas, en el que se aplicaban las características de los Servicios Diferenciados, se descartaban paquetes para que se cumplieran los contratos y para en el caso de dos colas servir una antes que otra, es decir, dependiendo del nivel de congestión, el tráfico de las colas de baja prioridad de salida es parcialmente descartado con el objetivo de **proteger** el tráfico de las colas de alta prioridad de salida.

A continuación, se muestra un resumen de los **resultados obtenidos**. Para el caso una cola (Plata) sin aplicar *DiffServ*, los resultados obtenidos son prácticamente los mismos tanto para la configuración "Mismo Contrato" como para la configuración "Distintos Contratos". Es decir, **no se tiene en cuenta los contratos de los clientes** a la hora de repartir el ancho de banda en exceso. Cuando todas las fuentes son TCP, el reparto del ancho de banda en exceso es **equitativo**, recibiendo cada cliente la cuarta parte del canal.
Cuando las fuentes son UDP y TCP, obtienen un mayor ancho de banda las fuentes UDP, los 3M a los que generan tráfico, ya que éstas no reducen su ventana de transmisión. Las fuentes TCP detectan la congestión y reducen su ventana de transmisión optando cada cliente TCP a conseguir en torno a 2M del ancho de banda del enlace final. Los resultados obtenidos para la configuración "Mismo Contrato" son prácticamente los mismos que cuando se aplican Servicios Diferenciados; es en las gráficas donde se aprecia el fenómeno de descarte.

Cuando se aplican Servicios Diferenciados y siendo todos los clientes TCP, los resultados obtenidos se corresponden con un **reparto equitativo** del ancho de banda no contratado para la configuración "Mismo Contrato". En la configuración "Distintos Contratos", **se tienen en cuenta los diferentes contratos de los clientes** y así, el reparto del ancho de banda en exceso es **proporcional** al ancho de banda contratado por cada cliente. El descarte de paquetes depende del contrato de cada cliente y de su ventana de transmisión. Es mayor cuanto menor sea el contrato. Cuando las fuentes son UDP y TCP, los clientes con menor contrato (UDP) no obtienen el menor ancho de banda como cabría esperar debido a que **se enfrenta tráfico TCP con tráfico UDP**. Obtienen un **mayor ancho de banda las fuentes UDP** ya que éstas no reducen su ventana de transmisión. Pero sufren mayor número de descarte que las fuentes TCP, por tener menor contrato y no reducir su ventana de transmisión. El descarte de los paquetes depende del contrato de cada cliente, de su ventana de transmisión y del tipo de tráfico UDP o TCP. Cuando se degradan las prestaciones de la red, (se ocupa el 80% del canal), TCP sufre más descartes que UDP, ya que al detectar congestión, reenvía los paquetes descartados. En la configuración "Distintos Contratos", se tienen en cuenta los diferentes contratos de los clientes y además el tipo de tráfico UDP o TCP para el reparto del ancho de banda en exceso.

Para el caso dos colas (Plata-Oro) sin aplicar *DiffServ* y siendo el contrato de los clientes **TCP mayor** que el de los clientes UDP, las fuentes obtienen un ancho de banda en exceso distinto en función del **peso de su cola** correspondiente (de su prioridad) y el tipo de tráfico UDP o TCP. Los clientes UDP consiguen los 3M a los que transmiten puesto que no se enteran de la congestión y continúan generando tráfico a la tasa máxima. Del ancho de banda total sobran 4M a repartir entre las fuentes TCP, que reducen su ventana de transmisión al detectar congestión, en función del peso de su cola correspondiente (de su prioridad), por lo que el reparto no es equitativo. **No se tienen en cuenta los contratos de los clientes**. Por tanto se obtienen prácticamente los mismos resultados cuando el contrato de los clientes **TCP es menor** que el de los clientes UDP.
Cuando se aplican Servicios Diferenciados y siendo el contrato de los clientes **TCP mayor** que el de los clientes UDP, las fuentes obtienen un ancho de banda en exceso distinto en función del peso de su cola correspondiente (de su prioridad), teniendo en cuenta los contratos y el tipo de tráfico UDP o TCP. Los clientes con menor contrato no obtienen el menor ancho de banda como cabría esperar debido a que se enfrenta tráfico TCP con tráfico UDP. Obtienen un mayor ancho de banda las fuentes UDP ya que éstas no reducen su ventana de transmisión. Pero sufren mayor número de descarte que las fuentes TCP, por tener menor contrato y no reducir su ventana de transmisión. El cliente de mayor contrato TCP C4 (2,6M) sufre numerosos descartes debido a que la cola Oro se desborda y el tráfico TCP se ve afectado a pesar de tener mayor contrato. Cuando el contrato de los clientes **TCP es menor** que el de los clientes UDP, las fuentes obtienen un ancho de banda en exceso distinto en función del peso de su cola correspondiente (de su prioridad), teniendo en cuenta los contratos y el tipo de tráfico UDP o TCP. Los clientes con menor contrato obtienen el menor ancho de banda. Obtienen un mayor ancho de banda las fuentes UDP ya que éstas no reducen su ventana de transmisión, y sufren menos descartes ya que tienen mayor contrato que las TCP. Las fuentes TCP no consiguen los 3M a los que transmiten porque tienen menor contrato que el tráfico UDP. El descarte de los paquetes depende del contrato de cada cliente, de su ventana de transmisión, del tipo de tráfico UDP o TCP y de la Clase de Servicio a la que son asignados. El cliente de mayor contrato UDP C3 (2,6M) sufre el menor descarte de todos los clientes.

Con estas pruebas se ha mostrado las posibilidades que ofrecen los Servicios Diferenciados del equipo Nortel *Passport 8600 Routing Switch* a la hora de garantizar contratos de manera justa y de repartir el ancho de banda en exceso del enlace final

Referencias

[1] Proyecto Final de Carrera “Estudio e Implementación de Mecanismos de Calidad de Servicio sobre una Arquitectura de Servicios Diferenciados”, autor Ricardo Alarcón Llamas, directora María Dolores Cano Baños.

[2] www.nortelnetworks.com/documentation

[3] “Calidad de servicio en IPv6”, disponible en http://long.ccaba.upc.es/long/050Dissemination_Activities/alberto_lopez_QoStutorial.pdf

[4] “Calidad de Servicio (QoS)”, disponible en www.uv.es/montanan/ampliacion/amplif_6.ppt

[5] “QoS y mecanismos de transición IPv4/IPv6”, Carlos Enrique Sedano Flores, Área de Ingeniería Telemática Universidad CARLOS III de Madrid.

[6] “Mecanismos que garantizan Calidad de Servicio en redes TCP/IP”, Luis Acuña, Alvaro Herrada, Carlos Juri, Felipe Morales, Universidad de Chile EL55A –Sistemas de Telecomunicaciones.

[7] “Diffserv como solución a la provisión de QoS en Internet”, Jorge Escribano Salazar, Carlos García García, Celia Seldas Alarcón, José Ignacio Moreno Novella, Departamento de Ingeniería Telemática, Universidad Carlos III de Madrid

[8] “EL PROTOCOLO DIFFSERV”, disponible en http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/549/8/T10471CAP2.pdf

[9] “CAPITULO II, Bases Teóricas”, Universidad Yacambú, disponible en: http://es.geocities.com/yvillasana2005/teg/Tesis/TrabajoEspecialdeGrado/CapituloII.htm

[10] “Evaluación de mecanismos de calidad de servicio en los routers para servicios multimedia”, disponible en http://informatica.uv.es/doctorado/SST/docto-2-qos.ppt

[11] “Introduction to Quality of Service (QoS)”, disponible en http://www.nortel.com/products/02/bstk/switches/bps/collateral/56058.25_022403.pdf

[12] Soluciones de seguridad de red extremo a extremo, disponible en www.nortelnetworks.com/security

[13] Passport 8000, 8600 Routing Switch Modules, disponible en http://www.bestdatasource.com/Nortel/datasheets/Pass_8000RSM.pdf

[14] Networking Concepts for the Passport 8000 Series Switch (part number 207307-D)

[15] Chapter 8 “Provisioning QoS networks”, Network Design Guidelines & Implementation Notes (part number 313197-B)

[16] Configuring QoS and Filtering for Ethernet Routing Switch 8600 R Modules, NN46205-507_318637-B_Rev_02.pdf

[17] “Configuración de QoS”, disponible en http://docs.us.dell.com/support/edocs/network/pc6024/sp/ug/configuh.htm

[18] “El papel de los acondicionadores de tráfico para ofrecer Calidad de Servicio extremo a extremo” disponible en http://repositorio.bib.upct.es/dspace/bitstream/10317/332/1/2004_AI_1.pdf.pdf

[19] “CBDQ: Garantía de Calidad de Servicio en Internet”, disponible en http://repositorio.bib.upct.es/dspace/bitstream/10317/925/1/cbdq.pdf

[20] Quality of Service in IP Networks, Karl Ahlin, disponible en http://www.ep.liu.se/smash/record.jsf?searchId=1&pid=diva2:18677

[21] Traffic Generator, disponible en www.caip.rutgers.edu/~arni/linux/tg1.html